HOCHSCHULE MITTWEIDA
University of Applied Sciences

Wissenschaftliche Berichte | Scientific reports

Konferenzband zum Scientific Track der Blockchain Autumn School 2024

Nr. 4, 2024

Konferenzband zum Scientific Track der Blockchain Autumn School 2024
Impressum

Herausgeber:
Hochschule Mittweida
University of Applied Sciences
Der Rektor
Prof. Dr. rer. oec. Volker Tolkmitt
Der Prorektor Forschung
Prof. Dr.-Ing. Uwe Mahn

Redaktion dieser Ausgabe:
Hochschule Mittweida |Referat Forschung
University of Applied Sciences

Leitung:
Prof. Dr.-Ing. Andreas Ittner
Dr. Dipl.-[Wi.] Ing. Volker Wannack

Kontakt:
Hochschule Mittweida
University of Applied Sciences
Referat Forschung
Postfach 1457
D-09644 Mittweida

Tel.: +49 (0) 3727 / 58-1264
Fax: +49 (0) 3727 / 58-21264
forschung@hs-mittweida.de
www.forschung.hs-mittweida.de

ISSN 1437-7624

Erscheinungsweise:
Unregelmäßig

Auflage:
Belegexemplare

Förderung:
Die Hochschule wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes.

Foto Titelseite: Hochschule Mittweida

Die Scientific Reports/Wissenschaftliche Berichte als Wissenschaftliche Zeitschrift der Hochschule Mittweida - University of Applied Sciences lösen die bisherigen Scientific Reports mit allen Volume I-III ab und erscheinen mit Nr.1, 1998 ab November 1998 in neuem Layout und in neuer Zählung.

Für den Inhalt der Beiträge sind die Autoren verantwortlich.

Im laufenden Kalenderjahr sind bereits erschienen:
Nr. 1, 2024
Messtechnische Überwachung von Stauanlagen
Nr. 2, 2024
Events als Treiber regionalökonomischer und touristischer Effekte
Nr. 3, 2024
24. Nachwuchswissenschaftler:innenkonferenz

SCIENTIFIC REPORTS | WISSENSCHAFTLICHE BERICHTE
The main aspect of the Scientific Reports is to promote the discussion of modern developments in research and production and to stimulate the interdisciplinary cooperation by information about conferences, workshops, promotion of partnerships and statistical information on annual work of the Hochschule Mittweida (FH) University of Applied Sciences. This issue will be published sporadically. Contributors are requested to present results of current research, transfer activities in the field of technology and applied modern techniques to support the discussion among engineers, mathematicians, experts in material science and technology, business and economy and social work.

Die Scientific Reports der Hochschule Mittweida sind online verfügbar unter:
www.forschung.hs-mittweida.de/veroeffentlichungen/scientific-reports

Eine Veröffentlichung einzelner Beiträge erfolgt entsprechend der Open Access Strategie der Hochschule Mittweida auf dem Hochschulschriftenserver: https://monami.hs-mittweida.de

INHALTSVERZEICHNIS

Airdrops as a governance tool for DAOs? An empirical analysis of voting participation

Marlene Marz
Hochschule Mittweida, Mittweida, Deutschland

Airdrops are a well-known incentive mechanism for blockchain protocols. In recent years, DAOs in particular have discovered "retroactive" airdrops that reward early adopters. This type of token distribution is also seen as a possible solution to the centralisation and lack of voting participation in DAOs. Therefore, 19 DAO airdrops were empirically analysed for their effect on governance activity. We compare the voting participation of airdrop recipients on Snapshot and (where available) on-chain with all token holders, as well as the delegation share. The participation of airdrop recipients was on average slightly higher than that of non-airdrop recipients, especially on Snapshot. We conclude that carefully designed airdrops can contribute to the overall governance strategy of DAOs.

1. Introduction

On 16 September 2020, the decentralised exchange Uniswap announced its own UNI token [1]. It was the first time that "free tokens" were issued on a large scale by a DAO ("Decentralised Autonomous Organisation"). Airdrops became particularly well known in the context of Initial Coin Offerings (ICOs) to promote projects [2]. However, Uniswap carried out a "retrospective" airdrop; the tokens were only issued to previous users. This type of airdrop offers little incentive for new users. Instead, Uniswap rewarded early supporters of the protocol. Retrospective airdrops are thus intended to appeal to intrinsically motivated users rather than users who specifically target airdrops ("airdrop farming") [2].

Regarding the governance function of tokens, airdrops in DAOs have another important feature: they distribute tokens to the community in a "decentralised" manner [3]. After all, the recipients are the initial "voter base" that will make decisions about the protocol in the future. This is particularly relevant given that many DAOs face governance challenges, such as unequal token distribution, strategic voting, or lack of voter participation [4].

But are airdrops an appropriate tool for increasing governance activity in DAOs? Previous analyses suggest that the majority of airdrop tokens are transferred or sold after a short time, with airdrops essentially being "free money" [5]. Accordingly, the effectiveness of airdrops in terms of governance is controversial. The aim is therefore to empirically analyse a group of DAO airdrops regarding the voting activity of the recipients. After characterising airdrops as an incentive mechanism in DAOs, we take a closer look at the methodology and selected airdrops (section 3). Section 4 then provides observations on the design of the airdrops, before presenting the results in section 5.

2. Airdrops as incentives

Incentives are a popular means of steering people's behaviour in a particular direction. As both sides benefit, incentives are considered ethically unproblematic, for example in contrast to penalties [6]. They are often financial in nature but can take many different forms. One could also speak of a kind of exchange ("trade") between two parties. On the other hand, an incentive always represents an extrinsic motivation; the recipient does not need to be "convinced" of the action or have a real interest in a product [6]. It is often assumed that non-profit organisations in particular have an incentive problem [7]. On the other hand, non-monetary incentives also shape human behaviour, e.g. social recognition [8].

DAOs are seen as a way to combine cooperative action and incentives [9]. This is largely due to the inherent properties of tokenisation. In many protocols, tokens are both a governance tool and part of the business model. They are also liquid and offer the prospect of price appreciation, unlike shares in 'traditional' collaborative structures. From this perspective, DAOs are more closely aligned with companies [10].

2.1. “Free money” & retrospective airdrops

Airdrops are probably the best-known incentive mechanism in the blockchain ecosystem [3]. In essence, they are the distribution of free tokens [11]. Fan et al. describe airdrops as a type of "digital coupon" that transfers tokens to a wallet [5]. Airdrops can incentivise early users to generate network effects, even if this means a large investment ("cold start problem") [11]. In contrast to companies, however, the tokens are to be understood as shares ("equity") rather than cash, because of ownership and governance rights.

There are many different airdrop design elements: some are passive, and you only qualify by owning a token ("token-based") or a wallet. Others are aimed specifically at users of competing protocols to win over users ("vampire attacks") [3]. These incentives were particularly prevalent in 2017 and 2018 when many ICOs took place. However, many of these projects were not sustainable or even turned out to be fraudulent. As a result, the reputation of airdrops declined [3]. The phenomenon resurfaced from around 2020 with the emergence of DAOs

that "retrospectively" distributed governance tokens [11].

Retrospective airdrops are better at rewarding early users and distributing the token more efficiently. They can be very targeted by tailoring them to on-chain criteria [3]. If an airdrop is not expected, this also prevents "airdrop hunting" or "farming". Today, however, few airdrops are actually "surprising". There is a lot of speculation, as some airdrops have proven to be very lucrative. A significant increase in activity is regularly seen in protocols where a governance token launch is possible [12].

Correspondingly, it can be observed that protocols have become stricter in their selection of participants. Airdrops linked to specific activities ("activity-based") are now the norm [3]. Allen even concludes that the protocols and airdrop hunters are in a kind of "co-evolutionary process" that is slowly making airdrops more sophisticated [2].

2.2. Airdrop Farming

Airdrop Farming refers to systematic participation in airdrops, sometimes even the creation of multiple accounts ("Sybils") to receive an airdrop multiple times [13]. This is a hindrance to the decentralisation of protocols and can give a false picture of how large or active a community is [5]. However, it is not easy to recognise or exclude airdrop farmers, especially before the distribution happens.

They can sometimes be detected by analysing the network of participating addresses. It is also typical for sybils that tokens from different addresses are accumulated on a wallet after the airdrop [13]. Some protocols therefore implement anti-sybil measurements, through identifying and excluding suspicious addresses (e.g., Hop Protocol) [13].

2.3. On DAOs

DAOs are a vibrant phenomenon across the web3. DAOs in their current form were first mentioned in a blog post by Ethereum co-founder Vitalik Buterin in 2014 [14]. Following the first large-scale DAO ("The DAO") in 2016, these on-chain organisations have evolved into a multifaceted form that serves various purposes beyond fundraising. DeepDAO, a DAO analytics service, now lists nearly 20,000 aggregated governments, which has multiplied in just a few years [15]. However, not all are active or meet the criteria of a DAO.

The fact that the number of DAOs is difficult to determine is also due to the fact that the DAO concept itself is controversial [16]. DAOs have already been described in the Ethereum whitepaper as "digital entities" whose members can determine the majority of code changes and spend money [17]. They are characterised by the fact that coordination takes place online and is implemented on a blockchain. While traditional organisations are usually hierarchical and tied to a presence or embedded in the legal system, the rules of DAOs are defined in smart contracts [18]. Technically, DAOs are a collection of these contracts [19].

For the purpose of this paper, we use the systematic definition of Rikken et al. derived from the key characteristics of DAOs:

> "A DAO is a system in which storage and transaction of value and notary (voting) functions can be designed, organized, recorded, and archived and where data and actions are recorded and autonomously executed in a decentralised way" [16]. "

2.4. Relevance

While much has been learned about governance systems in DAOs, there has been little analysis of the impact of airdrops on governance. In theory, airdrops decentralise token ownership, leading to a more balanced distribution and a larger base of voters [20]. More voters promise a better reflection of the community and give more weight to decisions. This would counteract plutocracy in DAOs. If the governance process is (more) decentralised and smaller token holders have a "voice", this in turn could positively increase voting activity [21]. In this way, airdrops could also counteract a lack of voting participation. An airdrop promotes user loyalty and can be an incentive for recipients to participate in the governance process and "give back" to the protocol [20].

However, there is little empirical evidence to support the assumption that airdrops are a governance tool. Previous analyses of airdrops tend to show that most recipients sell their tokens or leave the community. This means that the shares could even accumulate again. This paper therefore investigates the behaviour of governance voting. The research question is therefore: *What effect do airdrops in Decentralised Autonomous Organisations (DAOs) have, regarding the governance activity of the recipients?*

3. Methodology

To analyse the governance activity of airdrop recipients, the airdrop addresses are matched with the voters of the respective DAO (on Snapshot and on-chain).

The proportion of voting addresses is then compared to the governance activity of all token holders. This allows conclusions to be drawn about the activity of airdrop recipients compared to addresses that did not receive an airdrop. For better comparability, a set of DAO airdrops is used, in a period of six and twelve months after the airdrop, as well as at the time of analysis (October 2023).

3.1. Voting Retention

The “user retention” or “customer retention” is a well-known indicator used to assess the "stickiness" of users to a product or service [22]. For this purpose, the proportion of active or repeat users is calculated for a certain period [23]. This principle will also be used to analyse governance activity. We refer to this as the *"governance retention ratio"* or *"airdrop governance retention*

ratio". The proportion of token holders who participated in governance (in period t) is calculated as follows:

$$Governance\ Retention\ Ratio = \frac{Voter\ (t)}{Token\ Holders\ (t)}$$

For the proportion of airdrop recipients who took part in governance, the number of airdrop voters (in period t) is divided by the number of all airdrop recipients:

$$Airdrop\ Governance\ Retention\ Ratio\ = \frac{Airdrop\ Voter\ (t)}{Airdrop\ Recipients}$$

The data was accumulated using SQL queries on Dune Analytics [24]. Voting is based on data from Snapshot and (where applicable) on-chain voting data. Snapshot is an off-chain voting tool and the most widely used voting platform for DAOs, partly because of the (high) fees for on-chain transactions [25]. The platform only requires a wallet signature to verify the token ownership of the respective address, a "snapshot" of the authorised voters.

3.2. Selection of Airdrops

It's difficult to determine, how many DAOs have carried out an airdrop. Airdrops do not always leave traces "on-chain", for example when they are distributed via centralised exchanges. Even on-chain airdrops cannot always be recognised as such, e.g. to distinguish them from other payouts.

The DAO landscape, however, is much better mapped. On DeepDAO, the digital organisations can be sorted according to various criteria [15]. We decided to select the largest DAOs by treasury ("bank account" of the DAO) or number of "lifetime participants" (total number of voters to date), to include the most important DAOs in terms of financial strength and community. The number of proposals or votes were ruled out as criteria, as they are heavily dependent on how restrictive DAOs are with proposals and how long a DAO has been in existence.

To select the DAOs, a snapshot of DeepDAO was taken on 15 September 2023, including all DAOs with either a minimum of $25 million in assets or 5,000 lifetime participants. To exclude smaller bounties, at least 1% of the supply should have been distributed. In addition, the airdrop should be assigned to a clearly definable time period (criteria see Table 1).

Size	Airdrop	Data
Treasury of at least $25 million	At least 1% of the token supply reserved for the airdrop	Airdrop distributed on an EVM-chain (available on Dune Analytics)
Lifetime participants min. 5,000	Continuous airdrop, no vesting	Governance on Snapshot
	Airdrop publicly available	At least 1 proposal in each analysis period
	Airdrop of a governance token	

Table 1: Requirements for the airdrop selection

The following 19 airdrops were selected for analysis. Table 2 also shows the date (if available) until which airdrop recipients could qualify ("snapshot date"), the airdrop chain and the voting platform(s).

Selected Airdrops					
Protocol	Treasury	Particip.	Airdrop chain	Snapshot date	Voting
Treasury size and lifetime participants					
Optimism 1	3.1b	89k	Opt.	25.03.22	Optimism Agora
Arbitrum	2.8b	202k	Arb.	06.02.23	Snapshot, Tally
Uniswap	1.8b	30k	Eth.	01.09.20	Snapshot, Uniswap Gov. Portal
dydx	628m	4k	Eth.	26.07.21	Snapshot, dydx Gov. Portal
Ens	557m	88k	Eth.	31.10.21	Snapshot, Tally
Galxe	100m	40k	Eth.	28.04.22	Snapshot
Gitcoin	53m	13k	Eth.	01.04.21	Snapshot, Tally
Treasury size					
Frax	150m	1.4k	Eth.	20.02.22	Snapshot
Ribbon	84m	1.6k	Eth.	n/a	Snapshot
Euler Finance	49m	800	Eth.	21.03.22	Snapshot
Instadapp	45m	110	Eth.	16.06.21	Snapshot, Atlas
Hop	32m	1.8k	Eth.	01.04.22	Snapshot, Tally
Superrare	29m	600	Eth.	21.07.21	Snapshot
Thales Markets	25m	800	Eth.	06.09.21	Snapshot
Lifetime participants					
Swapr	n/a	18k	Arb. / Gnosis	01.07.21	Snapshot
Badger	5.8m	11k	Eth.	n/a	Snapshot
Open	n/a	11k	Polygon / Eth.	23.12.21	Snapshot
Ape	9.9m	8k	Eth.	n/a	Snapshot
Convex Finance	4.6m	5k	Eth.	23.04.21	Snapshot

Table 2: Selected airdrops

All the protocols in the dataset use Snapshot, except for Optimism. The protocol discontinued its use at the beginning of 2023 in favour of its own on-chain governance portal [26]. Eight protocols have implemented on-chain voting in addition to Snapshot. Some protocols have a two-stage voting process. Proposals must first be accepted on Snapshot ("temperature checks") before they go into on-chain voting. Uniswap even requires two Snapshot voting cycles before a proposal is qualified for on-chain voting [27].

A multi-stage voting process allows proposals to be revised again after the first vote. Others, e.g., ENS, make the voting platform dependent on the type of proposal.

They use additional on-chain voting only for proposals with fundamental protocol changes [28]. It is noticeable that it is mostly the larger protocols that have implemented on-chain voting. The DAOs from the data set, which were only selected via the lifetime participants, exclusively use Snapshot. All the protocols with on-chain voting also allow delegations or even actively promote them.

4. Observations on airdrop design

The selected airdrops were all retrospective, even if some of the distributions (e.g., Arbitrum) were anticipated [29]. This confirms the assumption that retrospective airdrops are particularly popular with DAOs [3]. In addition, all the airdrops were based on on-chain criteria ("activity-based") [3]. The selected airdrops started between September 2020 (Uniswap) and March 2023 (Arbitrum).

Among the selected airdrops, only Uniswap and Thales correspond to the "fair allocation" model (almost all addresses received the same amount). The remainder distributed individual amounts depending on the individual on-chain activity of the addresses ("differential allocation") [5].

4.1. Target groups

Three different target groups could be roughly recognized among the selected airdrops: Most of them were aimed at early adopters of their own protocol or product. Some of them qualified all users (e.g., Apecoin or ENS), while most protocols only whitelisted a subset of users. This approach is in line with the intention of rewarding early users and binding them to the protocol.

The second group were airdrops that specifically distributed tokens to users of another protocol to which they are connected. For example, Thales is a fork of Synthetix, and Convex was developed for users of Curve [30,31]. It can be assumed that they then give something back to the "partner protocols," but at the same time also intend to attract new users. Although this group of airdrops is retrospective, it is aimed at previously unknown users [11].

The third group shows a similar approach: some have distributed the airdrop to users of competing protocols (e.g., Instadapp or Badger). Here, too, a marketing motive can be assumed. It's also known as a "vampire attack" [3]. Contrary to what one might expect with retrospective airdrops, DAO airdrops are therefore not only used for the subsequent rewarding of their own users. Rather, some DAOs use the distributions to win over existing users of other protocols. Unlike most ICO airdrops, the on-chain activity can be used to select addresses with a potential fit for one's product [3].

4.2. Anti-Sybil measures

Airdrop farming is one of the biggest challenges for the protocols: The HOP Airdrop had a public "Sybil detection" programme. Using network analyses, the protocol excluded approximately 10,000 of the originally 43,000 authorised addresses from the airdrop ("blacklisting") [32].

In a further step, HOP called on its community to report airdrop farmers who had not yet been "discovered" themselves. The protocol also offered airdrop farmers the opportunity to report themselves for a smaller airdrop share [33].

Other airdrops (e.g., Arbitrum) even made use of HOP's Sybil list and excluded the same addresses from its airdrop [34]. Arbitrum and Optimism carried out their own network analysis as well, to identify patterns that indicate airdrop farming [35]. However, more detailed information on the procedure or the excluded addresses is not available, also to avoid accommodating airdrop farmers [36].

5. Results

All data, including the current status, can be found in the respective airdrop dashboards on Dune Analytics, which are linked here.

5.1. Airdrop size and distribution

The analysis of the 19 DAO airdrops shows that each airdrop is indeed individual. They vary greatly in terms of size and volume. This is also reflected in the voting activity. It is noticeable that some airdrops stand out from the others in terms of participating addresses (see Fig. 1).

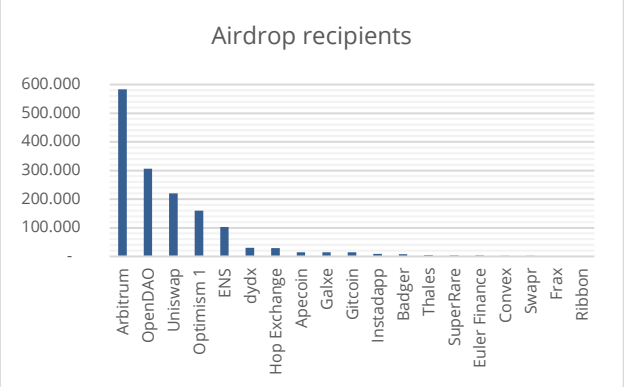

Fig. 1: Number of airdrop recipients

They also differ greatly in the supply that is made available for the airdrop. On average, it is around 11% of the total token supply. The exception is OpenDAO with 50% of the total supply.

5.2. Token distribution

Whether airdrops have a long-term impact on decentralization is controversial [5]. Based on the number of recipients, airdrops (initially) do have a "decentralising" effect in the sense that the token is widely distributed. An airdrop can add several (hundred) thousand token

holders to a project, which would otherwise not be possible, especially in the beginning. In almost all cases, the airdrop was a "genesis event" that heralded the launch of a governance token.

However, the sums distributed to the respective recipients are usually within a wide range. The widespread use of activity-based airdrops tends to reinforce this trend. Early users with high volumes sometimes receive very large shares.

In this analysis, the top 10% of the token recipients accounted for ~44% of the tokens on average, and for six of the selected airdrops, it was even more than half of the intended tokens. In the 1% percentile, an average of ~23% of the supply was distributed. The increased use of on-chain criteria (according to the “differential allocation” model) results in a more “unequal” distribution of tokens in this regard.

5.3. Actions after the airdrop

Even more important is what happens to the tokens after the airdrop. Previous studies have cast doubt on whether airdrops have a lasting effect [3]. In this analysis, only the situation at the time of the analysis (October 2023) was taken into account, regardless of how long ago the airdrops took place. This limits the comparability of the airdrops. The "oldest" airdrops in the dataset, Uniswap and Badger, have the highest transfer rates.

Nevertheless, the analysis shows that most recipients do not keep their tokens. On average, ~76% of recipients have now fully transferred their tokens and only ~12% still hold the tokens at the same address. The median "hodling" rate is only ~7%. Looking at OpenDAO, the high holding rate is more likely to be related to the low value of the token.

A transfer is not a confirmation of a sale, it could also be a transfer to a new wallet. However, it is reasonable to assume that the majority of the tokens have been sold - and therefore the recipients do not participate in the governance.

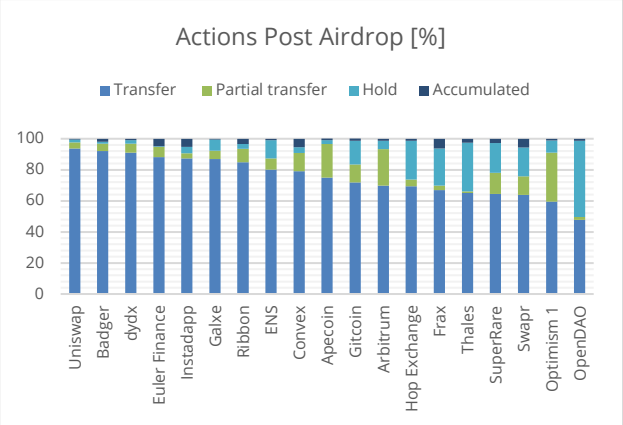

Fig. 2: Actions after the airdrop

5.4. Voting

The effect of an airdrop on participation is the core question of this paper. Both on Snapshot and on-chain, it can be seen that the DAOs are differently "active" in their governance in terms of the number of proposals. The airdrops with the fewest proposals (Swapr and Instadapp) also have comparatively low participation, while in reverse, this effect is not seen in the DAOs with many proposals. As Zhao et al. observed, too many proposals even can tend to favour voting fatigue [21]. A certain continuity in the proposals, on the other hand, is naturally a positive factor [21].

In absolute numbers (Snapshot and on-chain), participation differs greatly, with Optimism and Arbitrum standing out with over one million votes each. We can confirm Wang et al.'s assumption that activity in the ecosystem is concentrated on a small proportion of DAOs ("Pareto principle") [25]. The airdrops of these DAOs are also referred to as "high-profile airdrops" [37].

5.5. Snapshot voting participation

When looking at the Snapshot voting activity, a wide range is noticeable. On average, overall Snapshot participation has increased from ~8.2% after six months to ~9.7% in October 2023.

However, it is important to take a closer look at an individual case: The high level of participation in ENS is mainly due to one proposal. This was the ratification of the "ENS Constitution", which airdrop recipients were asked to sign during the claim process [38]. The voting frequency shows that around 91% of all ENS voters only voted once. The ENS Airdrop is therefore only comparable with the others to a limited extent.

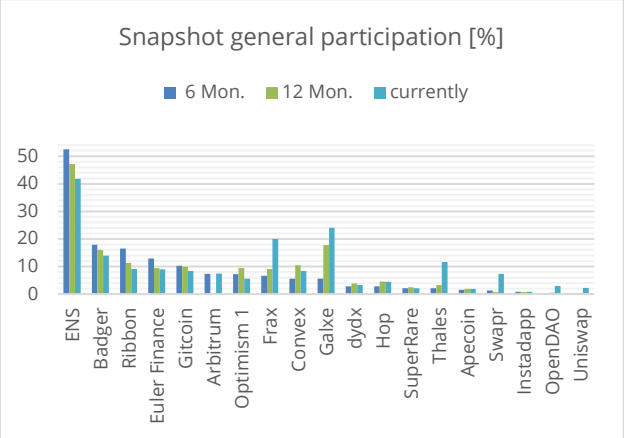

Fig. 3: Governance retention ratio

The proportion of airdrop recipients who voted on Snapshot is on average about 6% higher than the general participation in all time periods (~14% after six months and ~17% in October 2023). We therefore conclude that airdrop recipients in this dataset have increased overall voting participation. The airdrop governance retention rate is calculated from all airdrop recipients who have voted at least once. As a result, the value can only increase and does not reflect the 'loyalty' of the voters.

However, the voting frequency of airdrop recipients is very similar to that of all voters. In both groups, 45% of voters have voted at least three times.

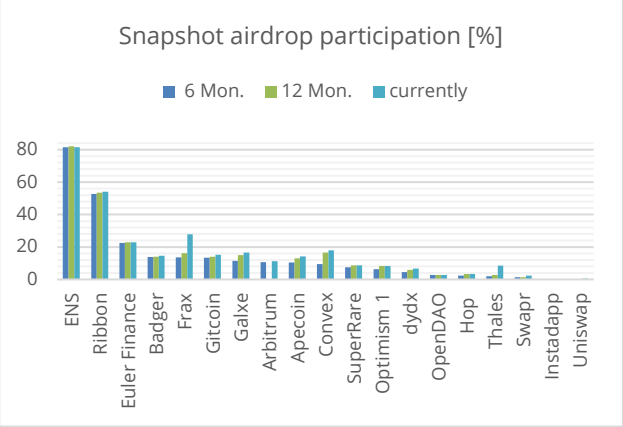

Fig. 4: Airdrop governance retention ratio

To see the effect of airdrop voters more clearly, we also calculated the governance retention ratio for voters excluding airdrop recipients, limited to the time of the analysis. Positive values indicate that a larger proportion of airdrop recipients were active in governance than token holders who did not receive an airdrop.

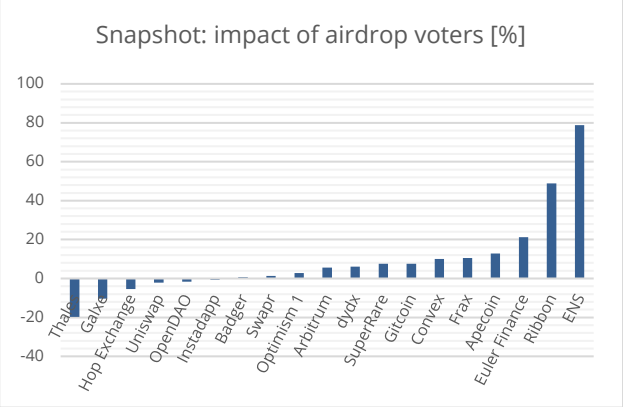

Figure 5: Difference between airdrop voters and voters excluding airdrop recipients

5.6. On-chain voting participation

Almost half of the analysed airdrops additionally use on-chain voting. The dominance of Optimism and Arbitrum is also noticeable here, with the most on-chain votes by far. The two DAOs each vote on their own protocol, while the other DAOs vote on Ethereum. The transaction fees could therefore contribute to the fact that the activity on the other DAOs is significantly lower. This is one of the reasons why delegations are widely used for on-chain voting.

The on-chain voting share is comparatively low or below the Snapshot share. The average value was 1.2% after six months 2.1% at the time of the analysis. Instead, on-chain DAOs largely refer to delegations, which are not included here (see. 5.5).

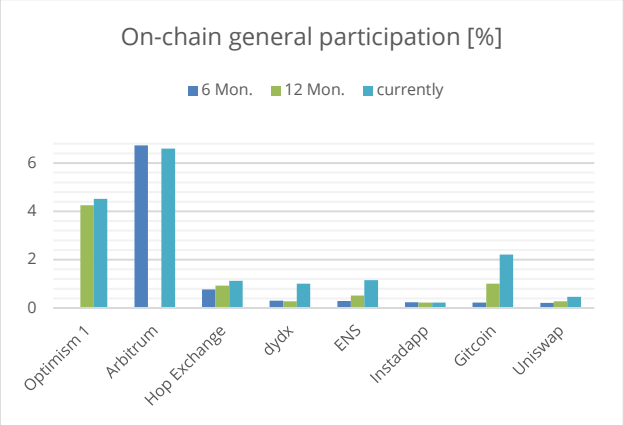

Fig. 6: On-chain governance retention ratio

The proportion of on-chain airdrop voters is slightly higher than that of the general public, ~1.7% after six months and ~2.6% in October 2023. Here, too, the figures are lower than on Snapshot.

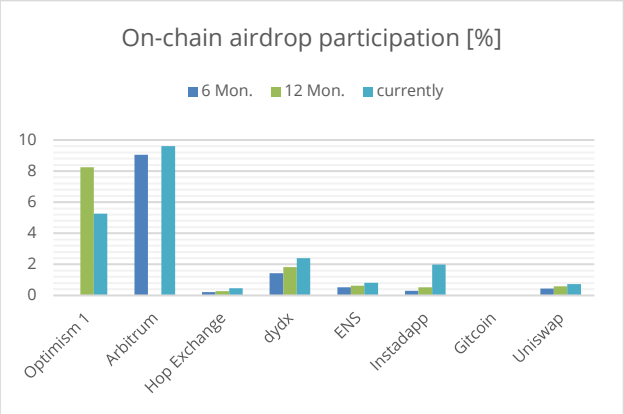

Fig. 7: On-chain airdrop governance retention ratio

5.7. A Note on Delegations

Delegating tokens is a popular way to "indirectly" increase voting participation [39]. The average token holder is typically unable to familiarise themselves with all the proposals and make an 'informed' decision each time [26].

This practice is particularly common in on-chain voting. Optimism, for example, now has over 600,000 addresses that have delegated tokens. Token holders can usually choose a delegate based on a public profile and transfer their voting rights. In most cases, due to the structure of governance contracts, delegation is even a prerequisite for voting [40]. Token holders must delegate to themselves in order to vote "directly".

The proportion of all token holders who have delegated their tokens at the time of analysis varies widely, from < 1% (dydx) to > 80% (HOP). In general, the delegation rate is much higher than the voting rate, averaging 35% after twelve months. Looking at airdrop recipients, the majority have delegated (54%). However, the higher proportion of airdrop recipients may be because some protocols required delegation at the time of airdrop request. These include ENS, Gitcoin and HOP, so the delegation

rate (at least one delegation event) among recipients for these airdrops is 100%.

"Mandatory delegations" may be a deliberate strategy to improve governance participation. Airdrop recipients have to decide whether to exercise their voting rights themselves or to pass them on.

5.8. Outlook

To better understand DAO airdrops, a number of things can be taken further in the analysis. These include a larger dataset, differentiating between the type of DAO or the role of the token in the protocol. It would also be interesting to look at DAOs that deviate from the one-token-one-vote model, such as NFT-based DAOs.

In terms of analysis, the voting behaviour could be analysed in more detail, e.g. whether small or large token holders show different patterns, or whether token holders are active in multiple DAOs in parallel. Finally, qualitative analysis could provide more insight into the characteristics of voters or airdrop recipients, who remain largely pseudonymous.

6. Conclusion: airdrops as a balancing act

We can confirm that retrospective and activity-based airdrops are widespread among DAOs [11]. Most of them are targeted at early users of the protocol, but some also reward external users of partner protocols, or of competing protocols.

But do airdrops serve as a governance tool? Token holder participation in governance is still the exception rather than the rule, especially on-chain. Only a small proportion of holders are active in voting over an extended period of time. Instead, protocols focus on delegations as a form of indirect participation.

Airdrop recipients on Snapshot had an average participation rate about 6% higher than that of token holders in general. This effect was smaller for on-chain voting (0.5%). Voting frequency was similar in both groups. Recipients also had higher delegation shares. *Accordingly, airdrops can be an instrument to increase governance activity.* However, the specific impact needs to be assessed on a case-by-case basis. In about a third of the protocols, the activity of the airdrop recipients was lower.

Airdrops - like any reward - are a balancing act: The aim is to decentralise the distribution of tokens and encourage general community engagement but also to reward active members in particular. A protocol's ability to find proportionality in the airdrop design may determine whether the airdrop achieves the desired goal.

Finally, incentives are only one piece of the puzzle in establishing a DAO long-term. After the initial impact of an airdrop, stable governance processes need to be established. Most importantly, a DAO should provide a useful product that is attractive even without additional incentives [5]. At best, the "extrinsic" motivation becomes an "intrinsic" one.

References

[1] Uniswap Labs Blog, Introducing UNI, Uniswap Protocol (2020). https://blog.uniswap.org/uni

[2] D. W. E. Allen, Crypto Airdrops: an Evolutionary approach, Social Science Research Network (2023). https://doi.org/10.2139/ssrn.4456248

[3] K. Lommers, C. Makridis, L. Verboven, Designing Airdrops, available at SSRN 4351000 (2023). http://dx.doi.org/10.2139/ssrn.4427295

[4] T. Barbereau, R. Smethurst, O. Papageorgiou, J. Sedlmeir, G. Fridgen, Decentralised Finance's Unregulated Governance: Minority Rule in the Digital Wild West, SSRN Electronic Journal (2022). https://doi.org/10.2139/ssrn.4001891

[5] S. Fan, T. Min, X. Wu, W. Cai, Altruistic and Profit-oriented: Making Sense of Roles in Web3 Community from Airdrop Perspective, arXiv (Cornell University) (2023). https://doi.org/10.1145/3544548.3581173

[6] R. W. Grant, The Ethics of Incentives: Historical Origins and Contemporary Understandings, Economics and Philosophy, 18 (2002), 111–139. https://doi.org/10.1017/s0266267102001104

[7] S. O. Borgen, Rethinking Incentive Problems in Cooperative Organizations, Journal of Socio-economics, 33 (2004), 383–393. https://doi.org/10.1016/j.socec.2004.04.010

[8] E. Fehr, A. Falk, Psychological Foundations of Incentives, European Economic Review, 46 (2002), 687–724. https://doi.org/10.1016/s0014-2921(01)00208-2

[9] J. Walden, Past, Present, Future: From Co-ops to Cryptonetworks, Andreessen Horowitz (2019). https://a16z.com/2019/03/02/cooperatives-cryptonetworks/

[10] A. Robey, What Co-ops and DAOs Can Learn From Each Other, FWB blog (2022). https://www.fwb.help/editorial/what-co-ops-and-daos-can-learn-from-each-other

[11] D. W. Allen, C. Berg, A. M. Lane, Why airdrop cryptocurrency tokens? Journal of Business Research, 163 (2023), 113945. https://doi.org/10.1016/j.jbusres.2023.113945

[12] Katte, The Gamble of Crypto Airdrop Hunting and What it Means for Blockchain Devs, Cointelegraph (2023). https://cointelegraph.com/news/the-gamble-of-crypto-airdrop-hunting-and-what-it-means-for-blockchain-devs

[13] Z. Liu, H. Zhu, Fighting Sybils in Airdrops, arXiv (Cornell University) (2022). https://doi.org/10.48550/arxiv.2209.04603

[14] V. Buterin, DAOs, DACs, DAs and More: An Incomplete Terminology Guide, Ethereum Foundation blog (2014).

https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide
[15] DeepDAO, DAO Analysis Service (n.d.). https://deepdao.io/
[16] O. Rikken, M. Janssen, Z. Kwee, The Ins and Outs of Decentralized Autonomous Organizations (DAOs), SSRN Electronic Journal (2021), 1. http://dx.doi.org/10.2139/ssrn.3989559
[17] Ethereum Whitepaper, A Next-Generation Smart Contract and Decentralized Application Platform (2024). https://ethereum.org/en/whitepaper
[18] Q. Wang, K. Liu, J. Li, Y. Yuan, L. Ouyang, F. Wang, Decentralized Autonomous Organizations: Concept, Model, and Applications, IEEE Transactions on Computational Social Systems, 6(5) (2019), 870–878. https://doi.org/10.1109/tcss.2019.2938190
[19] A. Wright, P. De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN Electronic Journal (2015), 15. https://doi.org/10.2139/ssrn.2580664
[20] Aragon Blog, How to Distribute a DAO Governance Token (n.d.). https://aragon.org/howto/distribute-a-dao-governance-token
[21] X. Zhao, P. Ai, F. Lai, X. R. Luo, J. Benitez, Task Management in Decentralized Autonomous Organization, Journal of Operations Management, 68 (2022), 649–674. https://doi.org/10.1002/joom.1179
[22] P. S. Fader, B. G. S. Hardie, How to Project Customer Retention, Journal of Interactive Marketing, 21 (2007), 76–90. https://doi.org/10.1002/dir.20074
[23] M. Viljanen, A. Airola, T. Pahikkala, J. Heikkonen, Modelling User Retention in Mobile Games, 2016 IEEE Conference on Computational Intelligence and Games (CIG) (2016). https://doi.org/10.1109/cig.2016.7860393
[24] Dune Docs, Welcome (n.d.). https://dune.com/docs/
[25] Q. Wang, G. Yu, Y. Sai, C. Sun, L. D. Nguyen, S. Xu, S. Chen, An Empirical Study on Snapshot DAOs, arXiv (Cornell University) (2022). https://doi.org/10.48550/arxiv.2211.15993
[26] Optimism Agora, Optimism Governance Platform (n.d.). https://vote.optimism.io/
[27] Uniswap Governance, Community Governance Process (2022). https://gov.uniswap.org/t/community-governance-process/7732
[28] ENS Docs, Governance Process (2024). https://docs.ens.domains/v/governance/process
[29] A. Gilbert, Arbitrum to Airdrop Long-Awaited ARB Token on March 23, The Defiant (2023). https://thedefiant.io/arbitrum-airdrop-set-for-march-23
[30] Thales, Thales Tokenomics: Introducing THALES Token, Medium (2021). https://thalesmarket.medium.com/thales-tokenomics-introducing-thales-token-3aab321174e7
[31] Convex Finance, Official Website (n.d.). https://www.convexfinance.com/
[32] Twitter Hop Protocol, Hop Protocol Updates (2022). https://twitter.com/HopProtocol/status/1522284561413160964?lang=de
[33] Hop-Protocol Github, Issues - Hop-Protocol/Hop-Airdrop (n.d.). https://github.com/hop-protocol/hop-airdrop/issues?page=1&q=is%3Aissue+is%3Aopen
[34] ArbitrumFoundation Github, GitHub – Arbitrum Foundation/Sybil-Detection (2023). https://github.com/ArbitrumFoundation/sybil-detection
[35] Arbitrum DAO - Governance docs, Sybil Accounts: A Conceptual Overview (n.d.). https://docs.arbitrum.foundation/concepts/sybil-account
[36] Optimism Docs, Airdrop 1 (2024). https://community.optimism.io/docs/governance/airdrop-1/#
[37] A. K. Shin, Airdrops: A Guide to Token Distribution & Rewards, Medium (2023). https://medium.com/@kaishinaw/airdrops-a-guide-to-token-distribution-rewards-7342271b328d
[38] ENS Youtube, How to Claim Your $ENS Airdrop (2021). https://www.youtube.com/watch?v=YOjRlzGz6yY
[39] World Economic Forum, Decentralized Autonomous Organization Toolkit, Insight Report (2023). https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf
[40] OpenZeppelin Docs, Governance (n.d.). https://docs.openzeppelin.com/contracts/4.x/api/governance

A Practical Model for Tokenizing Agricultural Assets: From Physical Commodities to Digital Futures Contracts

Deyan Paroushev
Sofia University St. Kliment Ohridski, Faculty of Mathematics and Informatics, Sofia, Bulgaria

Abstract: Small and medium-sized enterprises (SMEs) in agriculture face significant barriers to participating in institutional commodity trading, limiting their ability to manage risk and access global markets. This paper introduces a novel tokenized pooling mechanism that allows SMEs to collectively access over-the-counter (OTC) clearing services for agricultural futures. Leveraging blockchain technology, specifically Hyperledger Fabric, we create a transparent and efficient system for aggregating small-volume trades into standard-size contracts. Our model incorporates advanced pricing techniques that account for collateralization and cross-currency considerations. Implementation on Hyperledger Fabric demonstrates the feasibility of this approach in a real-world setting. Results indicate that this pooling mechanism can significantly reduce counterparty risk for SMEs while providing them access to institutional-grade risk management tools. This innovation has the potential to enhance market efficiency and promote more inclusive global agricultural trade.

Keywords: agriculture, tokenization, commodity futures, OTC clearing, Hyperledger Fabric

---

1. Introduction

The global agricultural commodity market, despite its vital role in the world economy, has long been characterized by inefficiencies and inequalities. Small and medium-sized enterprises (SMEs) in this sector, including family farms and local cooperatives, often find themselves at a significant disadvantage. These entities frequently struggle with limited access to sophisticated financial instruments, inadequate risk management tools, and difficulties in meeting the volume requirements of traditional futures contracts [1]. Such constraints not only impact their profitability but also hinder their capacity for growth and resilience in an increasingly volatile market environment.

In recent years, blockchain technology has emerged as a potential game-changer in various industries, and agriculture is no exception [2]. Tokenization, the process of creating digital representations of physical assets on blockchain platforms, offers a promising solution to address many of the long-standing issues faced by agricultural SMEs. By enabling fractional ownership of commodities and facilitating more fluid trading mechanisms, tokenization has the potential to democratize access to agricultural futures markets and enhance liquidity for smaller market participants [3].

Our research aims to bridge the gap between the theoretical potential of blockchain in agriculture and its practical implementation. We present a comprehensive model for tokenizing agricultural assets, with a specific focus on transforming physical wheat commodities into digital futures contracts. This model not only addresses the technical aspects of tokenization but also considers the unique challenges and requirements of the agricultural sector.

The primary objectives of this paper are to:

1. Develop a robust mathematical framework for the tokenization process, encompassing asset valuation, quality assessment, and mechanisms for fractional ownership.
2. Implement this model using Hyperledger Fabric, demonstrating its feasibility in a real-world blockchain environment.
3. Analyze the economic implications and potential market impact of the proposed tokenization platform, particularly for SMEs.
4. Explore the scalability and adaptability of the model to various agricultural commodities and market conditions.

By addressing these objectives, we seek to contribute to the evolving landscape of agricultural finance, offering a tangible pathway for SMEs to participate more effectively in global commodity markets. Our approach goes beyond simple digitization, incorporating sophisticated quality assessment mechanisms, risk management tools, and seamless integration with existing futures markets.

In the following sections, we will delve into the technical intricacies of our model, present the results of our implementation and testing, and discuss the broader implications for agricultural trade and finance. Through this research, we aim to pave the way for more inclusive, efficient, and resilient agricultural commodity markets,

leveraging the power of blockchain technology and tokenization to empower SMEs in an increasingly complex global economy.

2. Background and Literature Review

The intersection of blockchain technology and agricultural finance has garnered significant attention in recent years, promising to revolutionize how agricultural commodities are traded and financed. We start by examining the current landscape of agricultural tokenization, identifying gaps in existing approaches, and reviewing the relevant mathematical and technical foundations underpinning our proposed model.

2.1 Blockchain in Agriculture: Current State

Blockchain technology has found various applications in agriculture, from supply chain management to crop insurance. Notable initiatives include:

1. AgriDigital: An Australian platform using blockchain to create digital title for grains, enabling real-time payments and supply chain traceability.
2. AgriLedger: A platform that uses blockchain technology to enhance transparency and trust in the agricultural supply chain, allowing grain producers to track and verify their produce from farm to market, thereby ensuring fair pricing and improving trading efficiency.
3. GrainChain: A system that uses smart contracts to automate grain sales and payments, primarily targeting supply chain efficiency.

While these projects demonstrate blockchain's potential in agriculture, they primarily focus on supply chain management rather than addressing the specific needs of SMEs in futures markets.

2.2 Tokenization Models in Agricultural Finance

Several projects have emerged attempting to tokenize agricultural assets:

1. Agrotoken: Launched in Argentina, it allows farmers to tokenize their grain reserves as collateral for loans, enabling more flexible and efficient financial management for agricultural producers.
2. Cropto: A blockchain-based platform that facilitates direct trade between grain producers and buyers, offering transparency, security, and efficiency in transactions by leveraging digital assets.
3. AgriDex: A decentralized exchange platform that allows farmers to trade grain commodities using blockchain technology, providing a transparent and efficient marketplace.

These initiatives represent important steps towards digitizing agricultural assets, but they often lack sophisticated mechanisms for quality assessment, risk management, and integration with traditional futures markets.

2.3 Gaps in Current Approaches

Despite the progress made, several critical gaps remain in current tokenization models:

1. Limited Integration with Futures Markets: Most existing platforms do not provide a clear pathway for SMEs to participate in futures trading.
2. Inadequate Quality Assessment Mechanisms: Many models lack real-time, verifiable quality data integration, crucial for accurate asset valuation.
3. Insufficient Fractional Ownership Solutions: Existing platforms often struggle to efficiently pool small quantities of commodities to meet standard contract sizes.
4. Lack of Comprehensive Risk Management Tools: Current models often do not incorporate sophisticated risk assessment and hedging mechanisms tailored for agricultural commodities.
5. Limited Scalability Across Commodities: Many existing solutions are tailored to specific crops, lacking the flexibility to adapt to diverse agricultural products.

2.4 Mathematical and Technical Foundations

Our model builds upon several key mathematical and technical concepts to address these gaps:

1. Stochastic Processes in Commodity Pricing: We incorporate models like the Schwartz-Smith two-factor model to account for both short-term variations and long-term trends in commodity prices [4].
2. Quality-Adjusted Pricing Models: Our approach integrates multi-factor quality assessment into the pricing mechanism, drawing from established grading standards in the wheat industry [5].
3. Fractional Reserve Protocols: We adapt concepts from fractional reserve banking to create a robust pooling mechanism for small commodity quantities.
4. Smart Contract Architecture: Leveraging Hyperledger Fabric's permissioned blockchain environment, we implement complex business logic and access controls suitable for regulated financial markets.
5. Zero-Knowledge Proofs: To address privacy concerns in cross-border transactions, we explore the integration of zk-SNARKs (Zero-

Knowledge Succinct Non-Interactive Arguments of Knowledge) into our model.

By building upon these mathematical and technical foundations, our research aims to develop a more comprehensive and practical approach to tokenizing agricultural assets. This approach will address the identified gaps in current models and provide a robust framework for integrating tokenized commodities with traditional futures markets, ultimately empowering SMEs in the agricultural sector.

3. Mathematical Model for Tokenizing Agricultural Assets

In this section, we present a comprehensive mathematical framework for tokenizing agricultural assets, specifically focusing on wheat. Our model aims to bridge the gap between physical commodities and digital financial instruments, enabling smaller market participants to access futures markets more effectively. This framework closely aligns with our smart contract implementation on the Hyperledger Fabric platform, providing a robust foundation for practical application.

3.1 Asset Valuation and Quality Assessment Model

At the core of our tokenization process is an accurate valuation of the underlying wheat asset, accounting for both quantity and quality. We define the value $V(t)$ of a wheat asset at time t as:

$$V(t) = Q(t) * P(t) * QF(t)$$

Where:
$Q(t)$ is the quantity of wheat in metric tons, $P(t)$ is the current market price per ton, $QF(t)$ is a quality, factor based on multiple quality metrics

The quality factor QF(t) is calculated as:

$$QF(t) = min(PC/11, HFN/220, SW/76) * (1 + MA + BGA + IA)$$

Where: PC is the protein content (%)
HFN is the Hagberg Falling Number (seconds)
SW is the specific weight (kg/hl)
MA = (15 - MC) * 0.002 (Moisture Adjustment)
BGA = (4 - BG) * 0.001 (Broken Grains Adjustment)
IA = (2 - I) * 0.002 (Impurities Adjustment)
MC is the moisture content (%)
BG is the percentage of broken grains I is the percentage of impurities

Note: Wheat quality data taken from Euronext Milling Wheat Futures Contract No. 2 [6].

This quality factor model is implemented in the *calculateQualityFactor* function of our smart contract, ensuring that the tokenized value accurately reflects the physical wheat's quality characteristics.

3.2 Token Issuance Model

Once the asset value is determined, we model the token issuance process [7]. The number of tokens $N(t)$ issued at time t is given by:

$$N(t) = V(t)/T$$

Where T is the value represented by each token, set to 100 euros in our implementation. This one-to-one correspondence between tokens and physical wheat (1 token = 1 ton of wheat) simplifies the tokenization process and makes it more intuitive for market participants.

The token issuance process is implemented in the *TokenizeWheat* function of our smart contract, which creates a new Wheat token based on a Proof of Grain Reserve (PoGR) [8].

3.3 Pool Creation and Management Model

To facilitate the aggregation of smaller quantities of wheat, we introduce a pool model. A pool P is defined as:

$$P = W1, W2, \ldots, Wn$$

Where Wi represents individual wheat tokens. The total quantity of wheat in a pool QP is:

$QP = \Sigma\, Qi$ for $i = 1\ to\ n$

Where Qi is the quantity of each wheat token in the pool.

A pool is considered ready for contract creation when:

$$QP \geq 50\ tons$$

The quantity of 50 tons reflects Euronex requirement for the minimum quantity for creating a futures contract that would subsequently be traded on their platform. This model is directly implemented in the *AddToPool* function of our smart contract, which aggregates wheat tokens until the pool reaches the required threshold for futures contract creation.

3.4 Futures Contract Creation Model

When a pool meets the quantity threshold, a futures contract C is created:

$$C = ID, P, QP, PC, DD, S, SD$$

Where:
ID is a unique identifier
P is the associated pool
QP is the total quantity from the pool
PC is the contract price (initially set to 0)
DD is the delivery date (initially empty)
S is the contract status
SD is the settlement day (set to 10 days from creation)

This model is implemented in the *CreateEuronextContract* function of our smart contract, which generates a standardized futures contract based on the aggregated pool of wheat tokens.

3.5 Risk Metrics Model

To ensure robust risk management, we calculate risk metrics R for each wheat token:

$$R = V, VaR$$

Where: V is the volatility (set to 15% in our implementation) VaR is the Value at Risk, calculated as:

$$VaR = TI * V * \sqrt{(10/252)}$$

Where:
TI is the token's issued value 10 represents a 10-day VaR
252 is the number of trading days in a year

This risk assessment model is implemented in the *CalculateRiskMetrics* function of our smart contract, providing a standardized way to evaluate the risk associated with each token.

3.6 Price Discovery and Settlement Models

We incorporate two key pricing models to ensure accurate and fair price discovery:

1. Daily Settlement Price (DSP): $DSP = (\Sigma Pi * Vi)/(\Sigma Vi)$

Where:
Pi is the price of each recent trade
Vi is the volume of each trade

2. Exchange Delivery Settlement Price ($EDSP$): $EDSP = average\ of\ middle\ 50\%\ of\ last\ trading\ day\ prices$

These models are implemented in the *CalculateDailySettlementPrice* and *CalculateEDSP* functions of our smart contract, respectively. They ensure transparent and market-driven pricing mechanisms for our tokenized wheat assets.

3.7 Governance Model

To maintain a decentralized and democratic platform, we introduce a simple governance model where each token holder can vote on proposals:

$$Vote(P, TH) = For, Against$$

Where:
P is the proposal
$ID\ TH$ is the token holder ID

This governance model is implemented in the *GovernanceVote* function of our smart contract, allowing token holders to participate in key decision-making processes.

3.8 Ownership Transfer Model

To facilitate the transfer of ownership of wheat tokens, we define a transfer function:

$$T(W, O_{old}, O_{new}) \rightarrow W', TC$$

Where:
W is the wheat token being transferred
O_{old} is the current owner
O_{new} is the new owner
W' is the updated wheat token
TC is a transfer certificate recording the transaction

This model is implemented in the *TransferOwnership* function of our smart contract, ensuring secure and traceable ownership transfers.

3.9 Contract Execution Model

Finally, we define a model for executing the delivery of a futures contract:

$$E(C, P) \rightarrow C', W1', W2', \ldots, Wn'$$

Where:
C is the contract being executed
P is the associated pool
C' is the updated contract with delivery status
Wi' are the updated wheat tokens with new ownership

This execution model is implemented in the *ExecuteDelivery* function of our smart contract, facilitating the final step in the futures contract lifecycle.

3.9 Conclusion

This comprehensive mathematical framework provides a robust foundation for tokenizing wheat and integrating it with futures markets. By addressing asset valuation, quality assessment, token issuance, pool management, futures contract creation, risk assessment, price discovery, governance, and contract execution, our model offers a complete solution for bringing the benefits of digital finance to agricultural SMEs.

Each component of this model is directly implemented in corresponding functions within our Hyperledger Fabric smart contract, ensuring a seamless transition from theoretical framework to practical application. In the next section, we will delve deeper into the smart contract implementation, showcasing how these mathematical models are translated into executable code on the blockchain.

4. Smart Contract Implementation

In this section, we detail the implementation of our mathematical model for tokenizing agricultural assets using Hyperledger Fabric. Our smart contract, written in Go, translates the theoretical framework into a practical, blockchain-based solution. We'll provide an overview of key functions and then focus on a central function that exemplifies our approach.

4.1 Overview of Key Functions

Our smart contract implements the following key functions, each corresponding to a component of our mathematical model:

1. *TokenizeWheat*: Creates new wheat tokens based on Proof of Grain Reserve (PoGR).
2. *calculateQualityFactor:* Assesses the quality of wheat and calculates its value.
3. *AddToPool:* Aggregates wheat tokens into pools for futures contracts.

4. *CreateEuronextContract:* Generates futures contracts from completed pools.
5. *CalculateRiskMetrics:* Computes risk metrics for wheat tokens.
6. *CalculateDailySettlementPrice* and *CalculateEDSP:* Determine prices for settlement.
7. *GovernanceVote:* Enables token holders to participate in platform governance.
8. *TransferOwnership:* Facilitates the transfer of wheat tokens between parties.
9. *ExecuteDelivery*: Manages the delivery process for futures contracts.

Each of these functions plays a crucial role in realizing our tokenization model on the Hyperledger Fabric platform.

The class structure of our WheatToken smart contract, showcasing the key components and their relationships within the system is illustrated in Fig. 1. This diagram provides an overview of the contract's functionality, including token management, pooling, and order handling.

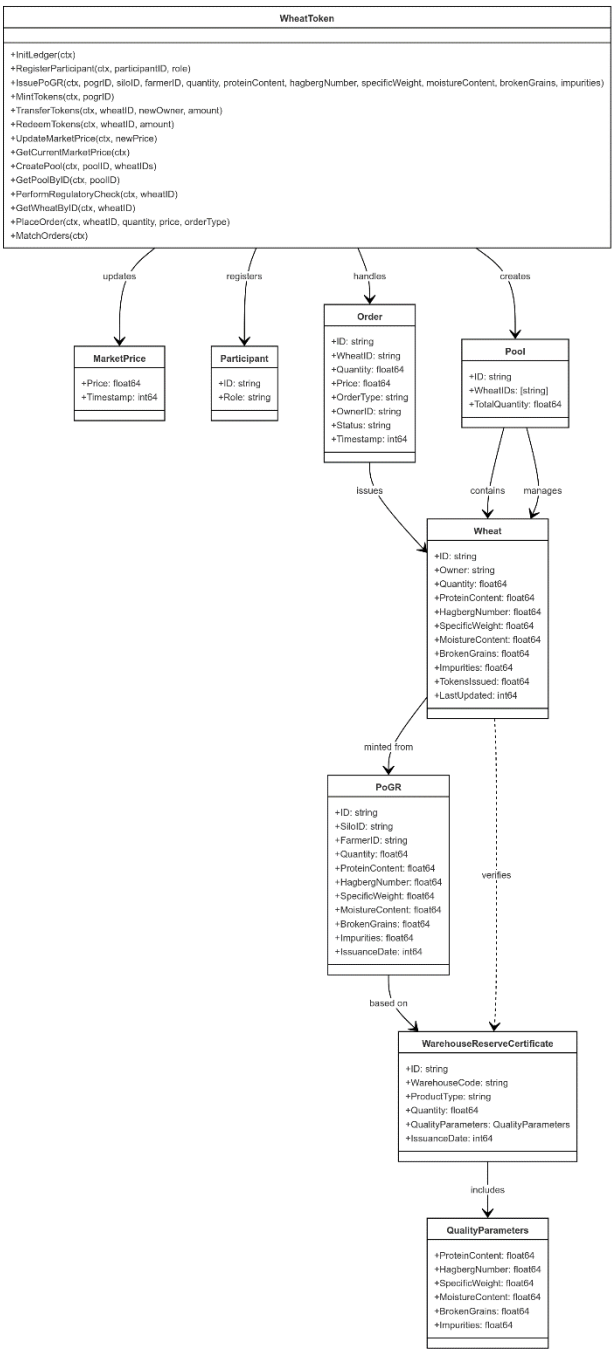

Fig. 1: WheatToken Smart Contract Class Diagram

The sequence of operations involved in creating and managing wheat futures contracts in our system can be seen in Fig. 2. It demonstrates the interactions between various components, from contract deployment to execution, highlighting the system's workflow.

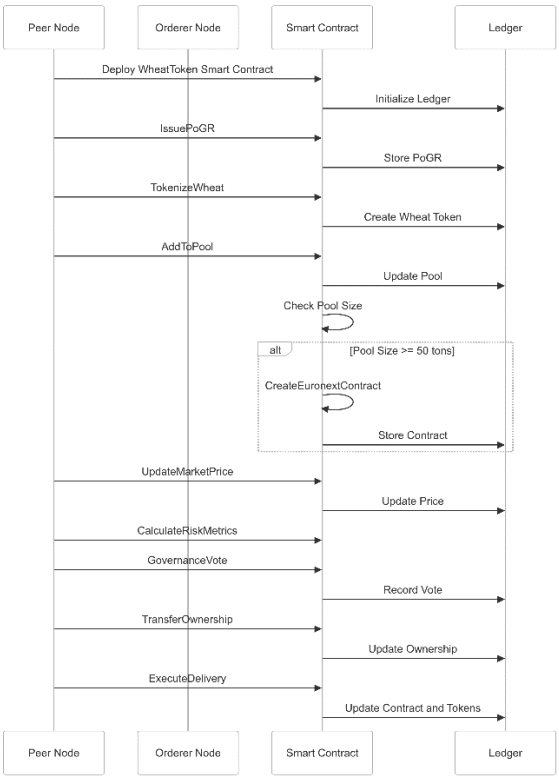

Fig. 2: Wheat Futures Contract Creation and Management Sequence Diagram

4.2 Deep Dive: AddToPool Function

The $AddToPool$ function is central to our implementation, bridging the gap between individual wheat tokens and standardized futures contracts. Let's examine this function in detail as presented in Fig. 3:

wheat_token.go

```go
// AddToPool adds a Wheat token to a pool
func (t *WheatForwardToken) AddToPool(ctx contractapi.TransactionContextInterface,
    poolID string, wheatID string, quantity float64) error {
    pool, err := t.GetPool(ctx, poolID)
    if err != nil {
        return err
    }

    wheat, err := t.GetWheat(ctx, wheatID)
    if err != nil {
        return err
    }

    if wheat.Quantity < quantity {
        return fmt.Errorf("insufficient wheat quantity")
    }

    pool.WheatIDs = append(pool.WheatIDs, wheatID)
    pool.TotalQuantity += quantity

    if pool.TotalQuantity >= 50.0 {
        pool.Status = "Ready"
    }

    poolJSON, err := json.Marshal(pool)
    if err != nil {
        return err
    }

    err = ctx.GetStub().PutState(poolID, poolJSON)
    if err != nil {
        return err
    }

    // Update wheat quantity
    wheat.Quantity -= quantity
    wheatJSON, err := json.Marshal(wheat)
    if err != nil {
        return err
    }

    return ctx.GetStub().PutState(wheatID, wheatJSON)
}
```

Fig. 3: *AddToPool* Function

This function embodies several key aspects of our model:

1. Fractional Contributions: It allows SMEs to contribute smaller quantities of wheat to a larger pool, addressing the challenge of meeting standard contract sizes.
2. Aggregation Mechanism: The function aggregates individual wheat tokens into a pool, tracking the total quantity and the constituent tokens.
3. Futures Contract Integration: When a pool reaches the threshold size (50 tonnes in this implementation), it automatically triggers the creation of a Euronext futures contract.
4. State Management: The function manages the state of both the pool and the individual wheat tokens on the blockchain, ensuring transparency and traceability.
5. Error Handling: Robust error checking ensures the integrity of the pooling process, preventing issues like insufficient quantities or duplicate entries.

The *AddToPool* function demonstrates how our mathematical model translates into practical code. It showcases the power of smart contracts in automating complex processes, from quality assessment to contract creation, in a secure and transparent manner.

4.3 Implementation Considerations in Hyperledger Fabric

In implementing our model on Hyperledger Fabric, we made several key design decisions:

1. State Management: We use Fabric's state database to store token, pool, and contract data, enabling efficient retrieval and updates.
2. Access Control: Hyperledger Fabric's built-in identity management is used to ensure that only authorized parties can execute sensitive operations like token creation or contract execution.
3. Chaincode Events: We emit events at crucial points (e.g., pool completion, contract creation) to facilitate real-time monitoring and integration with external systems.
4. Queries and Rich Queries: We implement complex queries to allow participants to efficiently retrieve information about tokens, pools, and contracts.
5. Privacy Considerations: While our current implementation operates on a shared ledger, Hyperledger Fabric's private data collections could be utilized in future iterations to enhance data privacy for sensitive information.

4.4 Conclusion

Our implementation in Hyperledger Fabric demonstrates the practical realization of our mathematical model for agricultural asset tokenization. By leveraging smart contracts, we've created a system that automates complex processes, enhances transparency, and opens up new opportunities for SMEs in agricultural futures trading. The *AddToPool* function, in particular, showcases how we've addressed the crucial challenge of aggregating smaller quantities of wheat into standard contract sizes, a key innovation in making futures markets more accessible to smaller players.

In the next section, we'll evaluate the effectiveness of this implementation in addressing the challenges faced by agricultural SMEs and compare it with traditional futures trading mechanisms.

5. Results and Discussion

5.1 System Implementation and Deployment

Our implementation of the *WheatForwardToken* smart contract on the Hyperledger Fabric network demonstrates the feasibility of a blockchain-based system for wheat futures trading. The Hyperledger Explorer dashboard for our wheat futures trading system, providing real-time insights into the blockchain's activity, including the number of blocks, transactions, and nodes is presented on Fig. 4.

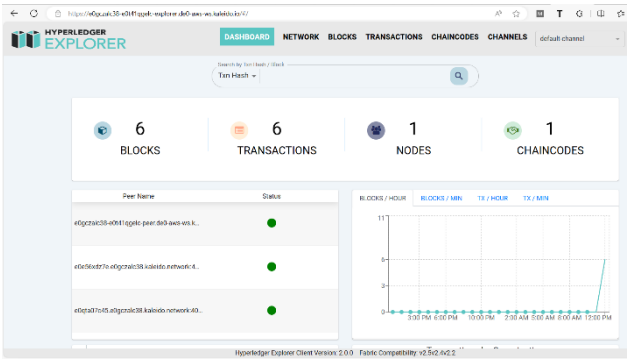

Fig. 4: Hyperledger Explorer Dashboard for Wheat Futures Trading System

The key components of our wheat futures trading system, illustrating how different modules interact to facilitate tokenization, price discovery, and regulatory compliance are outlines in Fig. 5.

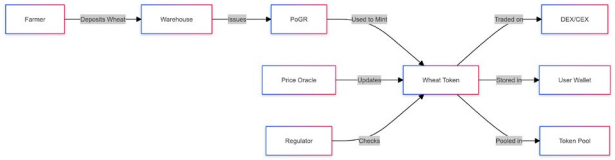

Fig. 5: Wheat Futures Trading System Components

The successful deployment is evidenced by the log entry found in the log files:

"2024-08-25 09:45:28.728 UTC 000f INFO[0m [orderer.common.server] [34;1mMain[0m -> Starting orderer:"

This confirms the initialization of the orderer node, a crucial component for maintaining consensus in Hyperledger Fabric. The system's architecture, as illustrated in Fig. 5, shows how various components interact to create a comprehensive tokenization platform.

5.2 Transaction Processing and Validation

As evident from the transaction details in Fig. 4, our system successfully processes both CONFIG and ENDORSER_TRANSACTION types, indicating its capability to handle system configurations and user-initiated actions

a) Transaction Types: We observe both CONFIG and ENDORSER_TRANSACTION types, aligning with typical Hyperledger Fabric operations. This diversity in transaction types indicates a fully functional system capable of handling both system configurations and user-initiated actions.

b) Validation: Transactions are consistently marked as VALID, confirming successful processing and consensus achievement. This is crucial for maintaining the integrity and reliability of the wheat futures trading system.

c) Chaincode Invocations: The "_lifecycle" chaincode is frequently invoked, indicating ongoing system-level operations related to chaincode lifecycle management. This suggests a dynamic and adaptable system capable of updating its smart contract logic as needed.

5.3 Tokenization Process and Token Lifecycle

The token lifecycle, illustrated in Fig. 6 (Wheat Token Lifecycle), demonstrates how our system addresses key challenges faced by SMEs in agricultural commodity trading, including fractional ownership and increased liquidity. The lifecycle of a wheat token in our system, from initial deposit to potential redemption, showcasing the various states and actions a token can undergo is depicted in Fig. 6:

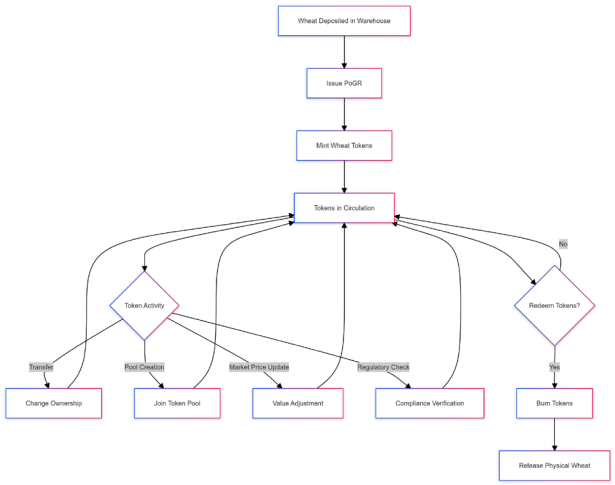

Fig. 6: Wheat Token Lifecycle

The tokenization process, as depicted on the same Figure, illustrates the journey from physical wheat deposit to digital token creation and circulation. This process addresses several key challenges faced by SMEs in agricultural commodity trading:

a) Fractional Ownership: By allowing the tokenization of smaller quantities of wheat, the system enables SMEs to participate in futures markets previously inaccessible due to volume constraints.

b) Liquidity: The ability to easily transfer and trade tokens, as shown in Fig. 2 (Wheat Futures Contract Creation and Management Sequence Diagram), potentially increases the liquidity of agricultural assets.

c) Price Discovery: The integration of a Price Oracle, as seen in Fig. 5 (Wheat Futures Trading System Components), contributes to more efficient and transparent price discovery for wheat futures.

5.4 Regulatory Compliance and Risk Management

The system incorporates several features to ensure regulatory compliance and effective risk management:

a) Compliance Checker: As shown in Fig. 5, a dedicated Compliance Checker module interfaces with regulatory data to ensure all transactions adhere to relevant regulations.

b) PoGR System: The Proof of Grain Reserve (PoGR) system, illustrated in Fig. 3, provides a crucial link between physical wheat deposits and digital tokens, ensuring the integrity of the tokenization process.

c) Regulatory Checks: Fig. 5 includes a "Regulatory Check" step in the token activity cycle, demonstrating the system's commitment to ongoing compliance.

5.5. Implications for SMEs in Wheat Futures Trading

The implemented system offers several potential benefits for SMEs:

a) Increased Market Access: In allowing fractional participation and pooling of resources (as shown in the "Join Token Pool" action in Fig. 6), SMEs can access futures markets that were previously out of reach.

b) Reduced Counterparty Risk: The use of smart contracts and blockchain technology, as evidenced by the transaction details in the Hyperledger Explorer, mitigates counterparty risk in cross-border transactions.

c) Enhanced Transparency: The immutable nature of blockchain transactions, combined with the system's integration of warehouse data and market data (Fig. 5), provides unprecedented transparency in wheat futures trading.

5.6 Limitations and Future Work

While our implementation demonstrates the potential of blockchain-based wheat futures trading, several limitations and areas for future work emerge:

a) Oracle Reliability: The dependence on external price feeds (Price Oracle in Fig. 5) introduces a potential point of failure or manipulation. Future work should focus on developing more robust and decentralized price discovery mechanisms.

b) Scalability: The current implementation, with limited nodes and transactions, leaves questions about the system's performance at scale. Further stress testing and optimization are necessary.

c) Regulatory Integration: While the system includes compliance checks, full integration with diverse regulatory frameworks across different jurisdictions remains a challenge to be addressed.

In conclusion, our implementation of a tokenized wheat futures trading system on Hyperledger Fabric demonstrates significant potential in addressing the challenges faced by agricultural SMEs. The system successfully combines blockchain technology with traditional financial instruments, paving the way for more inclusive and efficient agricultural commodity markets. However, further research and real-world testing are necessary to fully validate its effectiveness and impact on global wheat trading practices.

5.7 Technical Performance

The Hyperledger Explorer data, as shown in Fig. 4, provides insights into the system's technical performance. With 6 blocks created and 6 transactions processed, the system demonstrates its ability to handle basic operations. The presence of 1 active node and 1 deployed chaincode indicates a functional, albeit small-scale, implementation.

The transaction processing time, which averages around 3-4 seconds per transaction, suggests reasonable performance for a proof-of-concept system. However, further optimization would be necessary for large-scale deployment. The consistent creation of valid blocks, as seen in the Explorer, indicates the robustness of our consensus mechanism and the integrity of the blockchain.

5.8 Economic Impact

The implementation of our tokenized wheat futures trading system has the potential for far-reaching economic impacts, particularly for SMEs in the agricultural sector. By lowering barriers to entry for futures markets, our system could lead to more efficient price discovery and risk management for smaller producers. This improved market access may result in:

1. Enhanced income stability for farmers: With better hedging tools, SMEs can protect themselves against price volatility, potentially leading to more stable incomes and improved financial planning [9].
2. Increased market liquidity: The fractional ownership model could attract a larger number of

participants, potentially increasing market liquidity and reducing bid-ask spreads.

3. Reduced transaction costs: By disintermediating certain aspects of the futures trading process, our blockchain-based system could significantly reduce transaction costs, benefiting all market participants.
4. Improved capital allocation: With more accurate price signals and risk management tools, capital could be allocated more efficiently across the agricultural sector, potentially leading to increased productivity and innovation.
5. Greater financial inclusion: By enabling smaller producers to access sophisticated financial instruments, our system could contribute to broader financial inclusion in rural and developing areas [10].

While the full economic impact would require extensive real-world testing to quantify, these potential benefits suggest that our system could contribute to a more resilient and equitable agricultural economy.

5.9 Environmental Implications

Beyond its economic implications, our tokenized wheat futures trading system may also have positive environmental impacts. By creating a more efficient and accessible market for agricultural commodities, our system could contribute to reducing food waste and optimizing resource allocation:

1. Reduced overproduction: With better price signals and risk management tools, farmers may be able to more accurately match production to demand, potentially reducing overproduction and associated waste.
2. Optimized storage and transportation: The improved market access could lead to more efficient distribution of wheat, potentially reducing the need for long-term storage and minimizing transportation-related emissions.
3. Sustainable farming practices: As SMEs gain access to more sophisticated financial instruments, they may be better positioned to invest in sustainable farming practices, which often require upfront capital investment but offer long-term environmental benefits.
4. Resource allocation: The system's quality assessment mechanism could incentivize the production of higher-quality wheat, potentially leading to more efficient use of agricultural inputs like water and fertilizers.
5. Food security: By enabling more producers to participate in futures markets, our system could contribute to greater market stability, potentially enhancing food security and reducing the environmental impact of sudden supply shocks.

While these environmental benefits are potential outcomes, further research and real-world implementation would be necessary to quantify the actual environmental impact of our system. Nevertheless, these possibilities highlight the potential for blockchain-based agricultural finance to contribute to both economic and environmental sustainability.

6. Future Work

Based on our findings and identified limitations, we propose the following areas for future research and development:

1. Scalability Enhancement: Implement sharding techniques and optimize consensus algorithms to improve the system's capacity to handle a larger number of participants and transactions.
2. Decentralized Oracle Integration: Develop a decentralized price feed system to reduce reliance on single points of failure and enhance the reliability of market data.
3. Cross-chain Interoperability: Explore integration with other blockchain networks to facilitate cross-commodity trading and increase liquidity.
4. Regulatory Compliance Framework: Create a flexible compliance layer that can adapt to various jurisdictions' requirements, potentially utilizing zero-knowledge proofs for privacy-preserving compliance checks.
5. Advanced Risk Management Tools: Incorporate more sophisticated risk assessment models and hedging mechanisms tailored for agricultural commodities.
6. User Interface Development: Design and implement user-friendly interfaces for farmers, traders, and other stakeholders to interact with the system more easily.
7. Real-world Pilot Testing: Conduct extensive field tests with a diverse group of SMEs to validate the system's effectiveness and gather feedback for further improvements.

These future directions aim to address the current limitations of our system and expand its capabilities, ultimately working towards a more inclusive and efficient global agricultural commodity market.

Contact details

Sofia University St. Kliment Ohridski
Faculty of Mathematics and Informatics
Sofia, Bulgaria

E-Mail: dpparushev@fmi.uni-sofia.bg

ORCID: https://orcid.org/0009-0003-8231-8265

References

[1] N. Hryshchuk, “Financial initiatives in ensuring the investment activity of agricultural producers in the conditions of globalization challenges,” Three Seas Economic Journal, vol. 3, no. 1, pp. 59–67, Feb. 2022.

[2] M. Alobid, S. Abujudeh, and I. Szűcs, “The role of blockchain in revolutionizing the agricultural sector,” Sustainability, vol. 14, no. 7, p. 4313, Apr. 2022.

[3] M. Tarhini and Bucharest University of Economic Studies", “Application of asset tokenization, smart contracts and decentralized finance in agriculture,” Rev. Stud. Financ., vol. 6, no. 10, pp. 152–163, May 2021.

[4] J. S. Han, N. Kordzakhia, P. V. Shevchenko, and S. Trück, “On correlated measurement errors in the Schwartz–Smith two-factor model,” Depend. Model., vol. 10, no. 1, pp. 108–122, May 2022.

[5] J. Eum, I. Sheldon, S. R. Thompson, J. Eum, I. Sheldon, and S. R. Thompson, “Product quality in food and agricultural trade: Firm heterogeneity and the impact of trade costs.” Unknown, 2020.

[6] N. V. Euronext, “Technical specifications of the Milling Wheat NO.2 Futures contract,” 08-Aug-2024. [Online]. Available: https://live.euronext.com/sites/default/files/documentation/contract-specifications/Technical%20specifications%20of%20the%20Milling%20Wheat%20NO.2%20Futures%20July%202024.pdf.

[7] L. W. Cong, Y. Li, and N. Wang, “Token-based platform finance,” J. Financ. Econ., vol. 144, no. 3, pp. 972–991, Jun. 2022.

[8] Agrotoken, “Agrotoken White Paper,” 2020. [Online]. Available: https://cdn.prod.website-files.com/651d982d079d041f5fd45752/65de3cf04361dede1a5e92d2_EN%20-%20Agrotoken%20White%20Paper%202020.pdf.

[9] A. J. Arenas-Falótico, “Futures Contracts as a Means of Hedging Market Risks,” Aibi Revista De Investigación Administración E Ingeniería, vol. 11, no. 3, pp. 42–51, 2023.

[10] L.-Y. Tay, H.-T. Tai, and G.-S. Tan, “Digital financial inclusion: A gateway to sustainable development,” Heliyon, vol. 8, no. 6, p. e09766, Jun. 2022.

Blockchain in Aquaculture: Enhancing Sustainability and Transparency

Anastasia Platonava[1], Theofania Tsironi[2], Marc Cashin[1],
[1]Technological University of Shannon: Midlands Campus, Athlone, Ireland
[2]Agricultural University of Athens, Athens, Greece

This desk research explores current and prospective blockchain applications within the aquaculture sector. The primary aim is to create a theoretical foundation for deeper future research. Given the emerging nature of this topic, academic resources specific to blockchain use in aquaculture are limited. This paper reviews blockchain adoption in aquaculture, focusing on its role in tracking seafood supply chains and enhancing transparency and traceability. It highlights opportunities for advancing blockchain applications in aquaculture, including enhancing safety and quality control during critical stages such as transportation and distribution, as well as expanding its use for payments. This article provides a foundational understanding for stakeholders in aquaculture, policymakers and researchers, offering insights into the potential of blockchain to improve transparency, sustainability and efficiency within the sector. The findings also suggest directions for integrating advanced technologies, such as the Internet of Things (IoT), to further enhance the benefits of blockchain in aquaculture.

1. Introduction

Fish is one of the most traded food commodities globally, with over half of its exports originating from developing countries. Aquaculture significantly contributes to the Sustainable Development Goals (SDGs), such as Zero Hunger, by providing a sustainable source of protein and nutrition, Good Health and Well-being, through improved access to nutritious seafood, and Life Below Water, by promoting responsible management of marine resources and ecosystems. Additionally, it contributes to Decent Work and Economic Growth by generating employment and fostering economic development in coastal communities. Recent reports highlight aquaculture's tremendous potential to contribute to global food security and nutrition [1; 2].

As the fastest growing food supply sector globally, aquaculture plays a critical role in meeting the increasing demand for seafood, especially in the European Union (EU). In 2022, aquaculture production surpassed that of capture fisheries for the first time, claiming a 2% larger share of the total aquatic animal production [3].

Spain, France, Greece and Italy collectively accounted for more than two-thirds of the EU's aquaculture output volume in 2022 [4]. These countries have developed advanced aquaculture practices that not only bolster their economies but also contribute to regional food supplies. However, Asia dominates global aquaculture production, responsible for 88.3% of the total output, with China alone contributing 55.4% [3]. This concentration highlights the necessity for technological advancements and international collaboration to sustainably grow the industry.

Despite its growth, the aquaculture sector faces numerous challenges, including environmental concerns, supply chain inefficiencies, health and safety issues. Addressing these challenges requires innovative solutions to enhance sustainability and efficiency. Digital transformation is pivotal, leveraging technologies like IoT, AI (artificial intelligence) and big data to optimize production processes, reduce waste and monitor environmental conditions in real-time. These innovations not only enhance productivity but also establish robust traceability systems across the seafood supply chain.

Blockchain technology emerges as a transformative tool within this digital landscape, offering secure, immutable records of seafood transactions from source to consumer. By ensuring transparency and traceability blockchain strengthens consumer confidence, combats fraud and supports compliance with sustainability standards [5]. It addresses critical issues like illegal fishing, safeguarding marine ecosystems and promoting responsible seafood practices. Integrating digital technologies, including blockchain, into the seafood industry represents a shift towards sustainability, supporting global goals and ensuring a resilient supply chain for future generations [6].

This article explores the current challenges and limitations within the aquaculture industry and proposes how blockchain technology can be integrated to address these issues. It shows real-world blockchain applications in aquaculture and discusses the associated benefits. This paper aims to provide a foundation for stakeholders in aquaculture and seafood industries, policymaking and research to harness blockchain's potential across various facets of the fisheries sector.

This article is a result of the research secondment conducted within the ICHTHYS project - OptImization of novel value CHains for fish and seafood by developing an inTegrated sustainable approaCH for improved qualitY, Safety and waste reduction which has received

funding from the European Union's Horizon Europe Research and Innovation Programme under the grant agreement No.872217.

2. Background

Blockchain Technology

Blockchain technology has been called a pillar of the Fourth Industrial Revolution [7]. This revolutionary solution has been compared to the early rising of the Internet [8; 9].

This technology is intangible and invisible, making it difficult to describe. Conceptually, it can be pictured as a series of interconnected blocks, each containing information. The data within these blocks can be stored in various formats, such as text, images, or audio files [10; 11].

Fig.1: Structure of Blockchain

Blockchain technology was initially described in the early 90s, as a tool to timestamp digital documents, so to eliminate the possibility of backdating or tampering with them. In this case, blockchain may be seen as a "digital notary", digital notebook that lots of people can use and write in, with some special features that make it really secure and trustworthy [12].

In 2008, blockchain was revealed in a paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto (the pen name), so to create the digital cryptocurrency called Bitcoin. The initial idea behind blockchain is that it is a virtual database, which is used by Bitcoin and other cryptocurrencies for secure and anonymous transactions [13]. Since then, there was an emergence of other blockchain implementations, such as Ethereum and Hyperledger [14; 15]. Nowadays, blockchain technology is much more than just a tool to enable digital currencies, it is a platform, which has a nearly limitless amount of applications across almost every sector. It is a new global infrastructure that could transform many existing processes in business, governance and society [16].

Blockchain is a distributed system. It means that there is no central authority to hold the data and every computer on a network has a full copy of a blockchain (all blocks with all the stored information).

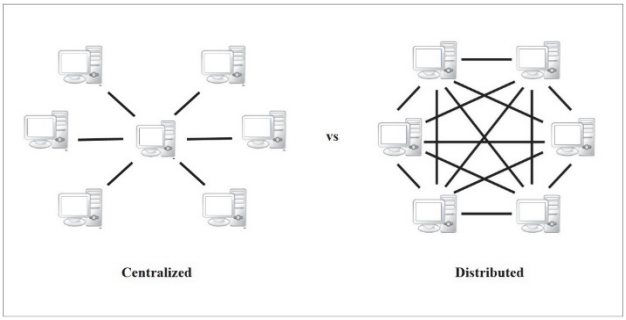

Fig. 2: Graphical View of the Distributed System to Understand Blockchain

When a new block is created, it is sent to every computer on a network, where it is verified and checked if it has not been changed. If everything is correct, all the computers will add this block to their own copy of a blockchain. If any block is invalid, it will be rejected and not added to a blockchain. It means that all the computers came to agreement that the block is valid. This process is called consensus, and Proof-of-Work may be called a consensus mechanism.

Figure 2 shows the difference between widely accepted centralized system and a peer-to-peer (decentralized) data infrastructure, in which information is distributed among all the nodes (participating devices: computers, smartphones) connected in the network. Every node is an "administrator" in distributed network, as mentioned earlier. It is very clear that main advantages of the decentralized system are speed, security and transparency.

Types of Blockchain

Let's have a look at Figure 3, that shows us four major types of blockchain systems which differ in governance and architecture.

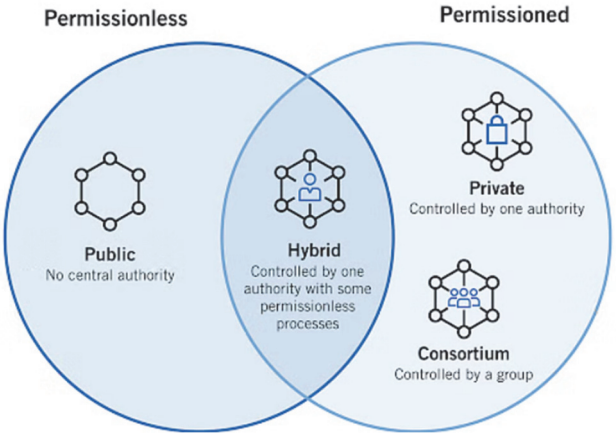

Fig. 3: Types of Blockchain

Public blockchain (Permissionless) – all records are opened to the public and everyone can take part in the consensus process. This type of blockchain is fully visible and decentralized with many thousands of confirming nodes present on the network. Immutability is high in this type of blockchain, but efficiency is low. Public blockchains are famous for its transparency feature. One of

the most popular examples of public blockchains is mining and exchanging cryptocurrencies like Bitcoin. Anyone with internet access can join the network, create a cryptocurrency wallet and receive/send transactions. Initially, that was Bitcoin cryptocurrency, which helped to popularize digital ledger technologies. Due to the nature of network, its openness and transparency, public blockchain is a good platform for social organizations and non-governmental institutions, which want to be trusted by public.

Private blockchain (Permissioned/Enterprise blockchain) – all information is available, but to a closed ecosystem. It often belongs to a specific organization, and only nodes coming from that organization are allowed to join the consensus process; however, it can also be created around a group of companies. It allows to distribute trust across companies, thus providing a more secure platform. In private blockchain only members have an access to the records (private access). Also, it can be organized in a way that organization, which set up this network, may decide who can view, add or change data. It is not a fully decentralized system, what may cause some sufferings and complications in case of a nodes failure. Permissioned blockchains are favoured by using centralized organizations, which leverage the strengths of the network for its business opportunities [17]. Use cases of private blockchains include, but are not limited to supply chain management, asset ownership, internal voting and trade secret management.

Consortium blockchain (Public/Permissioned blockchain or Federated blockchain) – a combination of private and public blockchains, in which a pre-selected group of users can participate in the consensus process, and not all users belong to the same organization. These participants are added individually as needed via some kind of authentication and authorization model. Immutability and efficiency are similar to the private blockchain, while consortium blockchain is intermediate in terms of centralization between the decentralized public blockchain and centralized private blockchain. Typically, in consortium blockchain, companies are distributed all around the world. Major use cases are banking and online payments, supply chain organizations.

Hybrid blockchain model/network – it is also a combination of both private and public blockchains. In this type of blockchain, some information about transactions would be made available to the public and some information would remain private. Simply speaking, information cannot be viewed by random third parties, but users can access it. Consortium blockchain allows users to share data by way of a specific authentication of individuals. The hybrid blockchain, on the other hand, will operate in a private context and then choose to add a subset of that private data back into a public blockchain network which is typically unpermissioned. Use cases of hybrid model include examples from the real estate, governmental and retail sectors, healthcare and financial services.

Every one of these types of blockchain has a particular use case or set of use-cases and should be selected carefully depending on the business model in question.

Challenges and Limitations in Aquaculture

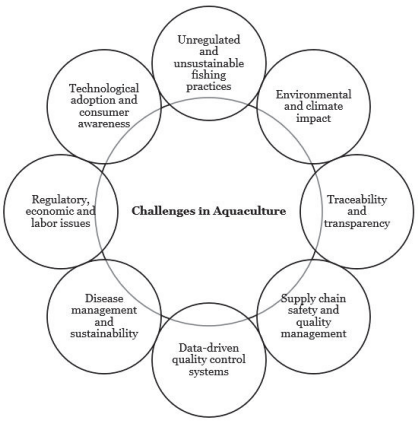

Fig. 4: Main Challenges in Aquaculture and Fisheries

Let's have a look at the Figure 4, that summarizes the main challenges in aquaculture.

Unregulated and Unsustainable Fishing Practices. Overfishing and illegal, unreported and unregulated (IUU) fishing practices remain a critical challenge in the aquaculture supply chain. It accounts for more than 700 kg stolen each and every second [18]. Consumption of aquatic products (both farmed and wild) is rising twice as fast as the global population [19]. This increase in demand leads to the harvesting of fish stocks beyond their natural reproduction rates, resulting in a significant reduction in marine resources. 89% of global wild fish stocks are overfished or being fully exploited [18]. Such practices often involve fishing without abiding to governmental and international regulations, such as fishing in protected zones. These unregulated activities not only lead to biodiversity loss but also result in fish being sold through black markets, thereby reducing the income of legitimate fishers. These issues directly impact the aquaculture industry by increasing competition for declining wild fish stocks, which are often used as feed in fish farming. The reduction of marine resources can drive up the cost of feed, making aquaculture less economically viable. Additionally, the biodiversity loss can disrupt ecosystems, affecting the health and growth rates of farmed species. As you can see from the Figure 5, IUU fishing activities negatively impact an overall aquaculture ecosystem.

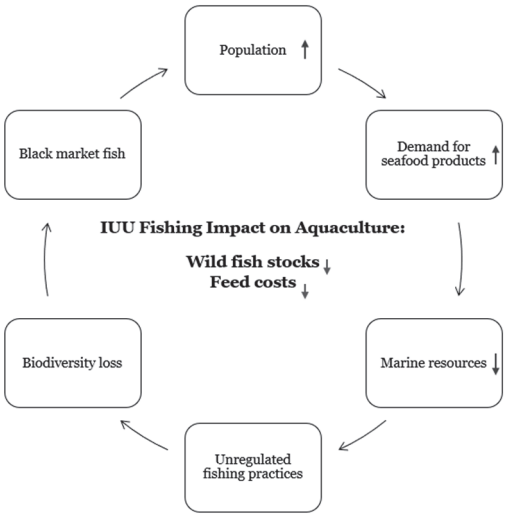

Fig. 5: Impact of unregulated fishing on aquaculture

Environmental and climate impact. Fishing is sustainable if it leaves enough fish in the oceans and minimises impacts on habitats and ecosystems [20]. However, the aquaculture industry faces significant environmental challenges, including pollution, habitat destruction and ecosystem imbalances. The United Nations Environment Programme (UNEP) has highlighted the problem of marine pollution and recognised it as a major driver of biodiveristy loss and ecosystem degradation [21]. Plastic marine debris, often originating from disposed or abandoned fishing nets, further contributes to ocean pollution. Additionally, climate change worsens these issues by changing ocean temperatures, sea levels and fish migration patterns, posing more risks to marine life.

To tackle the environmental and climate impact challenge in aquaculture, stakeholders must implement sustainable practices, including optimizing feed efficiency, adopting sustainable systems and ensuring proper waste and water quality management. Fish feed itself is the main contributor to environmental challenges in farmed Atlantic salmon aquaculture, highlighting the need for eco-labeling groups to prioritize reducing the environmental impacts of the feed supply chain [22]. Moreover, almost all aquaculture commodities depend on maintaining optimal water quality parameters, such as dissolved oxygen, temperature and pH, for successful cultivation calling for a robust system for quality control checks and maintaining these indicators throughout the production process.

Traceability and transparency. Traceability systems help identify and address issues related to production conditions, feed and storage, allowing for effective quality control and recalls.

There is an increasing concern of consumers about where their food is coming from [23]. Moreover, In light of the current global scenario, regulatory requirements, and stakeholder expectations for the aquaculture supply chain are more demanding than ever [24].

Transparency in aquaculture is crucial for stakeholder confidence. It enables to access detailed information about the origin, production practices and quality of the seafood, enhancing transparency and trust.

Seafood short-weighting, a less obvious but more prevalent issue, occurs when processors misrepresent the weight of seafood products by including the weight of excess ice (especially in frozen seafood) or additives. While adding ice or preservatives is a standard practice to keep seafood fresh, using excess amounts and including this added weight with the net weight of the seafood constitutes fraud. As a result, consumers end up paying more for less actual seafood due to short-weighting.

20% of seafood samples worldwide are mislabeled due to the fraud or human error [25]. In the aquaculture industry, *mislabeling seafood* can involve falsifying details like the species name and country of origin to bypass regulations, fees and business costs, using methods such as trans-shipping and falsifying trade documents to evade inspection and affect the pricing of responsibly farmed seafood.

Fig. 6: Full Aquaculture Chain Traceability

As a result of the complex globalized supply chains and the many different species in aquaculture, it becomes increasingly difficult to ensure traceability [26]. 60% of the seafood which comes from the ocean is discarded, lost or wasted in supply chains [18].

Supply chain safety and quality management.

In aquaculture, keeping fish and fish products safe and high-quality throughout the supply chain is a major challenge due to their perishable nature. From the time fish are harvested until they reach the consumer, they go through many stages that can impact their quality, including harvesting, cleaning, handling and preservation [27].

The supply chain for fish involves many players, such as fishermen, fish farm, middlemen, distributors, transporters, storage facilities, suppliers and retailers. Each step - transportation, distribution, retail display and domestic storage - poses risks to the fish's quality and safety. Factors like temperature changes, poor packaging, inefficient distribution, and improper handling can lead to spoilage and contamination.

Fish are typically transported at least twice: first from harvesting to processing facilities and then from packaging warehouse to distribution center, retail display and finaly domestic storage. Each transport stage presents additional challenges, making it crucial to manage conditions carefully [28].

To ensure fish products stay fresh and safe until they reach the consumption level, it is important to use effective preservation methods, maintain proper storage conditions, and manage transportation and distribution carefully. Addressing these issues helps protect the fish's nutritional value and safety, ensuring they meet consumer expectations and public health standards.

Implementing a system that can promptly notify all stakeholders in the supply chain if the quality of the fish is at risk is crucial for ensuring the integrity of the aquaculture sector.

Data-driven quality control systems. Fish freshness is one of the most important parameters in the fish market [29]. Errors in quality inspections lead to the distribution of poor-quality fish. Ensuring the safety and freshness of seafood products throughout the aquaculture supply chain requires robust data-driven quality control systems that can continuously monitor and verify conditions at every stage, from harvest to consumption. This also requires monitoring temperature conditions not only over pallets, but also boxes of food and individual packages at every step of distribution and storage [30]. Time-temperature integrators (TTIs), such as the 3M Monitor Mark, the TT Sensor, and CoolVu, are recognized for their effectiveness in managing cold chains. Implementing a unified system and technology that tracks all indicators of fish product quality can greatly benefit the aquaculture sector by ensuring comprehensive monitoring and consistency throughout the supply chain.

Disease management and sustainability. Contamination of the aquatic ecosystem and unhygienic handling practices along the fish supply chain can lead to a contaminated fish. Consumption of raw or under cooked fish and fish products is a major source of fishborne infections in humans [31]. Effective disease management is critical to mitigate these risks, which includes implementing hygiene protocols and monitoring for contaminants. Additionally, sustainable practices in aquaculture are essential to minimize environmental impact and support the long-term health of aquatic ecosystems.

Regulatory, economic and labor issues. The Guardian revealed that Asian slave labor is used in the production of prawns sold by major supermarkets in the US, UK and Europe [32]. In addition to human rights issues, there are economic implications, including the impact of unethical practices on market competitiveness and consumer trust. Improving transparency in supply chains and promoting ethical sourcing are crucial for ensuring that aquaculture products are not only economically viable but also socially responsible.

Technological adoption and consumer awareness. The adoption of advanced technologies in aquaculture faces challenges due to varying levels of technological readiness and investment across different regions. There is also a need for greater consumer awareness regarding the benefits of digital technologies. Consumers may lack understanding of how technology impacts the safety, quality and sustainability of aquaculture products, which can affect their willingness to support and pay a premium for products verified by these advancements.

3. Blockchain in Fisheries and Aquaculture

Present Applications of Blockchain in Fisheries and Aquaculture

Traceability system. The seafood industry has traditionally been characterised by a complex supply chain, which contrasts with other industries. Current traceability methods in this sector include digital labelling, excel spreadsheets, can printing, iPad data collection and pen and paper documentation. These methods create challenges in ensuring transparency and accountability among stakeholders such as fishermen, factories, certifiers and consumers.

Blockchain technology presents a solution to these challenges by enabling a shared and immutable ledger of truth among all stakeholders. This technology ensures that no party has the ability to change the information secretly, thereby enhancing trust and transparency across the supply chain. Blockchain facilitates secure traceability by allowing the entire chain of custody to be accessed, including critical social attributes such as fishing methods, vessel types and compliance data. Implementing blockchain builds a global peer-to-peer network that offers neutrality, reliability and security. It prevents the double-spending of certificates and claims without the need for a trusted third party. Blockchain serves as a fundamental layer of truth, providing a trusted reference point for all participants in the supply chain.

Fishery and aquaculture sectors may use blockchains to enhance traceability and transparency in value chains and to fight illegal, unreported and unregulated fishing. Blockchains in fisheries and aquaculture are mostly applied for traceability and to a lesser extent for payment or incentive [33]. Blockchain technology has proven to be an effective solution for addressing issues in aquaculture sector. The cryptographic security and decentralized structure of blockchain technology are particularly well-suited to establishing a trustless environment that enhances fisheries management. Fundamentally, the use of cryptographic proofs in blockchain can verify whether fishers and other participants in the supply chain adhere to government regulations and global market standards concerning sustainable practices and the quality of fish and seafood.

Several studies have reviewed the use cases and application of blockchain in seafood value chains and aquaculture [33; 34; 35]. Moreover, recent research has explored the combination of blockchain and IoT technologies in aquaculture, highlighting their potential to improve traceability, transparency and security within fish supply chain systems [36]. Smart contracts were investigated for their potential application in enhancing

traceability and transparency within fishery supply chains. One author proposed a blockchain-based fish traceability solution utilizing Ethereum smart contracts to manage processes across both wild-caught and farmed fishery supply chains [37].

A blockchain-based fish traceability system enhances trust by providing a transparent and unchangeable record of each fish product's journey, ensuring both authenticity and traceability. This level of transparency boosts consumer confidence, strengthens brand reputation and establishes credibility throughout the fishery supply chain.

Table 1 shows the worldwide implementation of blockchain technology in fishery and aquaculture. As it can be seen, there is a high representation of use-cases in the South-East Asia, including countries like Indonesia, Thailand and Fiji. This may be explained by the fact that improving traceability is critical in developing countries, the source of 90% of the world's seafood [18]. The developed countries that implement blockchain in their practices include Australia, Ireland, Norway, UK and USA.

Table 1 shows specific cases and purpose of the projects. Some projects are not limited to one country (such as Fishcoin and Provenance) as they try to operate worldwide.

Table 1: Summary of use cases of blockchain in fisheries and aquaculture worldwide

Country	Cases	Specific Purpose
Australia, South-East Asia: Indonesia, Singapore	Fishcoin	To build trust among stakeholders, to trace the journey of prawns from Australia to Singapore.
Ecuador (2019)	Sustainable Shrimp Partnership (SSP), IBM Food Trust	To provide transparency and traceability for its Ecuadorian farmed shrimp citing the rise of food fraud and poor-quality products entering the market [38].
Indonesia (2019)	Bumble Bee Foods	To track „Fair Trade" vertified yellowfin tuna.
Fiji (2017)	TraSeable Solutions, SeaQuest, World Wide Fund for Nature (WWF) – New Zealand, ConsenSys	To create a completely transparent and traceable supply chain, utilising innovative blockchain technology, for the fresh and frozen tuna supply chain [39].
Indonesia (2016), UK	International Pole & Line Foundation (IPNLF), WWF, Humanity United)	certifications, to prevent duplicating or falsifying the information, form the basis for an open system for traceability powering consumer-facing transparency.
Ireland 2021	Verifact, Aldi	To capture all information from catch through to the retail shelves [40].
Ireland (2021), UK (2022)	A: Verifact, BIM Ireland; B: Verifact FIS Scotland	A: To capture full supply chain data in wild capture hake and farmed salmon in the Irish seafood sector [41]. B: Nephrops and Haddock.
Mexico	SeaBos (leading actor: Nutreco)	To track volume of sardines caught per harvest and address undocumented fishermen aboard vessels.
Norway	The Norwegian Seafood Association - Sjømatbedriftene, IBM Food Trust, Atea	To record data such as the catch location and time, storage temperature, shipping updates, customs clearance, and fish feed details, among other things.
Netherlands	"Check Your Fish"	To provide transparency into the origin.
Switzerland (2018)		To launch its MSC-certified tuna products with a QR code for blockchain [42].
Thailand (2018)	Pacifical, A-tato	To track fish destined for canning.
USA (2019)	Raw Seafoods, IBM Food Trust	To create a fully traceable supply chain focused on scallops [43].
Australia (2019), Worldwide	OpenSC (leading actors: WWF-Australia, BCG Digital Ventures)	To improve traceability of Patagonian toothfish and to see its movement through the supply chain.

In developing countries, there is a predominant focus on small-scale operations involving individual fishermen, whereas developed countries prioritize large-scale industrial operations at the industry level. This disparity is largely influenced by economic conditions, regulatory frameworks and historical and cultural practices within each respective region.

Circular fishing nets and gear. The integration of blockchain technology in the recycling of fishing nets and gear represents a significant advancement in promoting transparency and accountability in the supply chain. Blockchain enables precise tracking and tracing of fishing nets and gear from their use on vessels to their eventual recycling and repurposing into new commercial products. This not only helps ensure the responsible disposal and reuse of fishing materials but also supports

broader environmental conservation efforts by reducing ocean pollution.

An innovative project in the seafood industry is Net 360, an Irish blockchain-enabled initiative aimed at repurposing and recycling fishing nets [44]. Developed in collaboration with Verifact, Net 360 uses blockchain technology to track the lifecycle of fishing nets from their time on commercial vessels through their disposal and recycling processes. This system ensures that the nets are responsibly managed and provides transparency at each stage, allowing businesses and consumers to verify that the materials they use or purchase are sourced sustainably.

Another significant effort is an international ocean conservation group Sea Shepherd's Ghost Network. This project focuses on recovering abandoned fishing gear from the oceans. Then it is repurposed or recycled, with the entire process being traceable through blockchain technology.

The success and value of these projects is evident as the automotive industry has started incorporating recycled sea plastics into their manufacturing processes. Companies like BMW and Ford are now using recycled materials in their vehicle components [45; 46].

Tokenisation of aquaculture assets. Tokenization is the process of converting real-world assets (such as fish stocks or aquaculture facilities) into digital tokens that exist on a blockchain [47]. It introduces a new way to invest and allows for fractional ownership, making aquaculture projects more accessible to a wider range of investors. Stobox, a tokenization company, is helping ICM Capital tokenize the world's largest shrimp farm in the Middle East while promoting sustainable aquaculture practices [48].

Payments and incentives. Only two use-cases have been identified in terms of the use of blockchain as a payment and as a direct delivery of incentives to fishers. Fishcoin project a token ecosystem mechanism, meaning that seafood producers and intermediaries are rewarded (with tokens, or digital vouchers) for providing data onto the platform [49]. Fishers can then use the Fishcoins to pay their bills or to buy minutes for their phones [33].

Another use-case is the Tracey project, created by TX using the Streamr marketplace platform, uses blockchain to help small-scale fishers in developing countries gain access to financing [50].

Centralized and decentralized finance. Only one application of blockchain has been found in relation to CeFi or DeFi). Tracey project facilitates microfinance through decentralized and centralized finance lenders, expanding financial access to underrepresented micro SME markets globally. The project aims to enhance creditworthiness assessments and overcome geographic barriers, ultimately improving the livelihoods of small-scale fishers and contributing to global poverty reduction efforts.

Potential Development Directions for Blockchain in Fisheries and Aquaculture

Overall, the majority of blockchain use cases reviewed are concentrated in the wild fishing industry rather than in aquaculture as a distinct sector. Blockchain technology has been predominantly applied in developing countries such as Fiji, Thailand and Indonesia, where it supports small-scale fisheries. In contrast, developed countries like Ireland, Norway, UK and USA utilize blockchain on a broader industry-wide scale. While most blockchain projects focus on wild fish species such as tuna, salmon and scallops, there are fewer applications specifically targeting aquaculture, with current use cases primarily involving salmon and shrimp. Non-governmental organizations (NGOs) often play a crucial role in these initiatives.

Although the involvement of small-scale fisheries in blockchain projects shows promise, larger companies in developed nations need to enhance their transparency efforts. The primary application of blockchain technology in the examples provided is to improve transparency and traceability within seafood supply chains. This includes tracking seafood from its origin to the consumer, ensuring data integrity and preventing fraud through open and secure systems.

However, the use of blockchain remains limited in critical stages where safety and quality are most vulnerable, such as transportation, distribution, retail preservation and handling processes. This represents a significant area for further exploration and development. Similarly, while data-driven control systems, like temperature monitoring, have potential, their current applications are restricted. Integrating Internet of Things and other advanced technologies could greatly enhance these systems' capabilities in the future. This data helps in identifying disease outbreaks early, tracking the spread and implementing targeted interventions. As such, there are opportunities to move in this direction.

Additionally, the application of blockchain as a payment method in the seafood industry has been minimal. This presents another opportunity for growth, where blockchain could streamline and secure transactions, especially in cross-border trade.

There is a growing interest in sustainable plastics recycling, particularly with the use of blockchain technology, as demonstrated by initiatives such as Verifact's Net 360 project in Ireland and Sea Shepherd's Ghost Network. The increasing focus on sustainability, driven by pressing legislation and the SDGs, further underscores the need for innovative solutions. This trend towards integrating blockchain in recycling could provide valuable insights and opportunities for aquaculture to adopt similar approaches, improving sustainability and efficiency in the sector.

Conclusion

Blockchain technology is not universally applicable and is not suited for every industry or problem. It is essential for companies and individuals to carefully define their objectives and thoroughly evaluate the specific benefits that blockchain can offer. While blockchain holds significant potential for enhancing transparency, traceability and efficiency in the aquaculture industry, a provocative question arises: *„Do companies, corporations and fishers genuinely want to embrace such a high level of transparency?"*

An important consideration for future research is whether blockchain might become a regulatory requirement or a standard within the aquaculture industry. If blockchain were to be named as a baseline standard for all stakeholders, it could fundamentally change the landscape of industry practices, ensuring standardization in transparency and accountability. Such a development would require widespread adoption and adaptation, impacting how businesses operate and comply with regulations.

In this context, the potential enforcement of blockchain as a standard may prompt stakeholders to reconsider their willingness to fully disclose operational details and practices. As the industry contemplates these possibilities, it is crucial for stakeholders to assess how blockchain could integrate into their operations and the implications of potential regulatory changes. Understanding both the current applications and future regulatory scenarios will be essential for leveraging blockchain effectively while addressing its challenges.

Contact details

Contact person: Anastasia Platonava
E-Mail address:
A00226775@student.tus.ie
ORCID: 0000000186560743s

References

[1] OLABİNJO, O., & OPATOLA, S. (2023). Agriculture: A Pathway to Create a Sustainable Economy. Turkish Journal of Agricultural Engineering Research, 4(2), 317–326. https://doi.org/10.46592/TURKAGER.1348187
[2] UN. (2024). Food security and nutrition and sustainable agriculture | Department of Economic and Social Affairs. https://sdgs.un.org/topics/food-security-and-nutrition-and-sustainable-agriculture
[3] FAO. (2024). The State of World Fisheries and Aquaculture 2024. In The State of World Fisheries and Aquaculture 2024. FAO. https://doi.org/10.4060/cd0683en
[4] European Commission. (2024). Aquaculture statistics. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Aquaculture_statistics&oldid=611980
[5] Burke, T. (2019). How blockchain is changing the supply chain conversation. https://www.ift.org/news-and-publications/food-technology-magazine/issues/2019/june/features/how-blockchain-is-changing-the-supply-chain-conversation
[6] Rowan, N. J. (2023). The role of digital technologies in supporting and improving fishery and aquaculture across the supply chain – Quo Vadis? In Aquaculture and Fisheries (Vol. 8, Issue 4, pp. 365–374). KeAi Communications Co. https://doi.org/10.1016/j.aaf.2022.06.003
[7] World Bank. (2019). Blockchain: How the Fourth Industrial Revolution can help accelerate progress towards development. https://www.worldbank.org/en/news/feature/2019/01/24/blockchain-como-asegurarse-que-cada-dolar-llegue-a-quien-lo-necesita
[8] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol.
[9] Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.2580664
[10] Antonopoulos, A. M. (2010). Mastering Bitcoin : unlocking digital crypto-currencies.
[11] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, 557–564. https://doi.org/10.1109/BIGDATACONGRESS.2017.85
[12] Anastasia Platonava, & Marc Cashin. (2023). Blockchain Applications in the European Higher Education Arena. https://www.forschung.hs-mittweida.de/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1715736354&hash=059a69f6723acf4d875e355c6430e3ac9ae8c8fc&file=fileadmin/verzeichnisfreigaben/forschng/dokumente/Scientific_Reports/Scientific_Reports_2023/Sc_Report_2023_02-Blockchain.pdf
[13] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org
[14] Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
[15] Cachin, C., Schubert, S., & Vukolić, M. (2017). Non-determinism in Byzantine fault-tolerant replication. Leibniz International Proceedings in Informatics, LIPIcs, 70, 24.1-24.16. https://doi.org/10.4230/LIPIcs.OPODIS.2016.24
[16] WEF. (2018). Building Block(chain)s for a Better Planet. https://www3.weforum.org/docs/WEF_Building-Blockchains.pdf
[17] Hameed, B. I. (2019). Blockchain and Cryptocurrencies Technology: a survey. JOIV : International Journal on Informatics Visualization, 3(4), 355–360. https://doi.org/10.30630/joiv.3.4.293
[18] Fishcoin. (2024). Fishcoin: Blockchain Based Seafood Traceability & Data Ecosystem. https://fishcoin.co/#fishcoin-ecosystem
[19] FAO. (2022). Record fisheries and aquaculture production makes critical contribution to global food security. https://doi.org/10.4060/CC7285EN
[20] MSC. (2023). What Is Overfishing | Marine Stewardship Council. https://www.msc.org/what-we-are-doing/oceans-at-risk/overfishing
[21] UNEP. (2024). Marine Pollution. https://www.unep.org/topics/ocean-seas-and-coasts/regional-seas-programme/marine-pollution

[22] Sherry, J., & Koester, J. (2020). Life Cycle Assessment of Aquaculture Stewardship Council Certified Atlantic Salmon (Salmo salar). Sustainability 2020, Vol. 12, Page 6079, 12(15), 6079. https://doi.org/10.3390/SU12156079
[23] FAO. (2014). Policy and governance in aquaculture Lessons learned and way forward.
[24] Luna, M., Fernandez-Vazquez, S., Tereñes Castelao, E., & Arias Fernández, Á. (2024). A blockchain-based approach to the challenges of EU's environmental policy compliance in aquaculture: From traceability to fraud prevention. Marine Policy, 159, 105892. https://doi.org/10.1016/J.MARPOL.2023.105892
[25] Oceana. (2015). 1 in 5 Seafood Samples Mislabeled Worldwide, Finds New Oceana Report - Oceana USA. https://usa.oceana.org/press-releases/1-5-seafood-samples-mislabeled-worldwide-finds-new-oceana-report/
[26] Winkelhuijzen, R., & Van Burik, M. (2016). A Horizon Scan on Aquaculture 2015: Traceability.
[27] Parimi, S., & Anusha, S. (2018). Agility in the Factors Effecting the Quality and Safety of Fish Products. Indian Journal of Commerce & Management Studies, IX(2), 1. https://doi.org/10.18843/IJCMS/V9I2/01
[28] VKM. (2008). Opinion of the Panel on Animal Health and Welfare of the Norwegian Scientific Committee for Food Safety Transportation of fish within a closed system Norwegian Scientific Committee for Food Safety.
[29] Prabhakar, P. K., Vatsa, S., Srivastav, P. P., & Pathak, S. S. (2020). A comprehensive review on freshness of fish and assessment: Analytical methods and recent innovations. Food Research International, 133, 109157. https://doi.org/10.1016/J.FOODRES.2020.109157
[30] Taoukis, P. S., & Tsironi, T. N. (2018). Time–Temperature Integrators (TTI). In Reference Module in Food Science. Elsevier. https://doi.org/10.1016/B978-0-08-100596-5.21872-6
[31] Bedane, T. D., Agga, G. E., & Gutema, F. D. (2022). Hygienic assessment of fish handling practices along production and supply chain and its public health implications in Central Oromia, Ethiopia. Scientific Reports 2022 12:1, 12(1), 1–11. https://doi.org/10.1038/s41598-022-17671-5
[32] The Guardian. (2014). Revealed: Asian slave labour producing prawns for supermarkets in US, UK, Thailand. https://www.theguardian.com/global-development/2014/jun/10/supermarket-prawns-thailand-produced-slave-labour
[33] Tolentino-Zondervan, F., Ngoc, P. T. A., & Roskam, J. L. (2023). Use cases and future prospects of blockchain applications in global fishery and aquaculture value chains. Aquaculture, 565, 739158. https://doi.org/10.1016/J.AQUACULTURE.2022.739158
[34] Vijay, T. A., & Raju, M. S. (2023). Blockchain Applications in Fisheries. E3S Web of Conferences, 399. https://doi.org/10.1051/e3sconf/202339907008
[35] Blaha, F., & Katafono, K. (2020). Blockchain application in seafood value chains. FAO. https://doi.org/10.4060/ca8751en
[36] Ismail, S., Reza, H., Salameh, K., Kashani Zadeh, H., & Vasefi, F. (2023). Toward an Intelligent Blockchain IoT-Enabled Fish Supply Chain: A Review and Conceptual Framework. Sensors, 23(11). https://doi.org/10.3390/s23115136
[37] Patro, P. K., Jayaraman, R., Salah, K., & Yaqoob, I. (2022). Blockchain-Based Traceability for the Fishery Supply Chain. IEEE Access, 10, 81134–81154. https://doi.org/10.1109/ACCESS.2022.3196162
[38] FishFocus. (2019). Sustainable Shrimp Partnership Demonstrates Success | Aquaculture. https://fishfocus.co.uk/sustainable-shrimp-partnership-demonstrates-success/
[39] WWF. (2018). New Blockchain Project has Potential to Revolutionise Seafood Industry | WWF. https://wwf.panda.org/wwf_news/?320232/New-Blockchain-Project-has-Potential-to-Revolutionise-Seafood-Industry
[40] Verifact. (2022c). Supply Chain Validation and Telling the Consumer Story. https://vfact.com/case-studies/aldi
[41] Verifact. (2022b). Net360. Implementing blockchain traceability to add value to end of life fishing nets. https://vfact.com/case-studies/net360
[42] Gustav Gerig. (2018). Tuna blockchain with QR code. https://www.gerig.ch/en/sustainability/blockchain/
[43] IBM. (2019). Raw Seafoods Collaborate to Use Blockchain to Help Improve Seafood Traceability and Sustainability While Addressing Fraud. https://newsroom.ibm.com/2019-10-17-IBM-Raw-Seafoods-Collaborate-to-Use-Blockchain-to-Help-Improve-Seafood-Traceability-and-Sustainability-While-Addressing-
[44] Verifact. (2022). Net360. Implementing blockchain traceability to add value to end of life fishing nets. https://vfact.com/case-studies/net360
[45] DesignNews. (2021). Ford Snares a New Source of Plastics in Recovered Fishing Nets. https://www.designnews.com/automotive-engineering/ford-snares-a-new-source-of-plastics-in-recovered-fishing-nets
[46] PlasticsToday. (2021). BMW Treads Sustainable Path with Recycled Fishing Nets. https://www.plasticstoday.com/automotive-mobility/bmw-treads-sustainable-path-with-recycled-fishing-nets
[47] Zhang, Y., Gong, B., & Zhou, P. (2024). Centralized use of decentralized technology: Tokenization of currencies and assets. Structural Change and Economic Dynamics, 71, 15–25. https://doi.org/10.1016/J.STRUECO.2024.06.006
[48] Stobox. (2024). Tokenization in the Desert. Aquaculture in Qatar with Stobox. https://blog.stobox.io/tokenization-in-qatar-with-icmcapital-stobox
[49] Pita, C. (2023). REPORT ON THE MAIN IMPEDIMENTS AND POTENTIAL INCENTIVES FOR SEAFOOD BLOCKCHAIN DEPLOYMENT. http://www.sea2see.eu/
[50] Streamr. (2021). Tracey integrates with Binance Smart Chain ecosystem enabling DeFi lending for micro SMEs. https://blog.streamr.network/news-tracey-integrates-with-binance-smart-chain-ecosystem-enabling-defi-lending-for-micro-smes/

Requirements for a blockchain-based proof of origin for green hydrogen

Tobias Wappner, Alexander Grünewald, Maik Hausmann
Fraunhofer IML, Dortmund, Deutschland

Hydrogen produced from renewable energy, so called green hydrogen, is seen as a key element of the energy transition in Germany. So far, however, a green hydrogen economy is barely developed, industrial applications require restructuring, are cost intensive and lag, while the pursued ecological benefit of transitioning to hydrogen technology is difficult to prove. Blockchain is a promising technology here. It offers the potential to trace the origin of hydrogen and thus contributes to document sustainable business practices. This paper examines requirements for a blockchain-based proof of origin for green hydrogen by carrying out a literature review and deriving requirements from the data found. In total, 11 requirements are found to be crucial to establish a working solution. While future research on how to overcome these challenges is needed, the benefits of a blockchain-based solution outweigh traditional approaches, which are lacking both standardization and transparency.

1. Introduction

The energy landscape is transforming significantly as the global search for sustainable energy solutions intensifies. This shift is driven by technological innovations and an increasing commitment to environmental protection [1]. A central element of Germany's strategy to combat climate change is the energy transition, which aims to meet the electricity demand entirely from renewable sources by 2045 [3]. Hydrogen, as a green energy carrier, plays a central role in this transformation [4].

Hydrogen, known for its high energy content and environmentally friendly combustion, is emerging as a promising alternative to conventional fossil fuels. Since its oxidation produces only water, hydrogen significantly reduces carbon emissions and promotes the development of energy storage technologies [5]. The European Union has also adopted this approach for the European market, introducing the EU Hydrogen Strategy in 2020 [6].

Currently, hydrogen is used as a process gas in various industrial sectors. Different methods for hydrogen production exist, such as electrolysis or steam methane reforming [7]. Depending on the production method, hydrogen is assigned a color, indicating the associated greenhouse gas emissions. Green hydrogen, in particular, plays a crucial role in the energy transition, as it is produced through electrolysis using renewable energy sources like wind and solar power, making it potentially emission-free [8, 9].

Current forecasts predict that by 2050, up to 23% of the total energy consumption in the EU will be supplied by hydrogen [10]. In Germany alone, this will require electrolysis capacities in the double-digit gigawatt range [11]. However, a significant portion of Germany's hydrogen demand will need to be met through imports in the medium to long term. The German government anticipates a national demand for hydrogen and its derivatives of 95 to 130 TWh by 2030, with approximately 50 to 70% (45 to 90 TWh) expected to be imported [12].

Substantial challenges in production, storage, and logistics along the hydrogen supply chain must be overcome to fully exploit the potential of hydrogen [5]. Production capacities and supply chains need to be newly established in many areas. The decentralized production of hydrogen and increasing international imports also heighten the need for transparency regarding the origin of hydrogen and its derivatives [13, 1].

Parallel to these developments in the hydrogen sector, complementary technologies that promote establishing a sustainable hydrogen economy are gaining increasing focus. Notably, blockchain technology offers extensive potential for digitizing the supply chain [14]. Due to its inherent properties, its application in the hydrogen market, especially for the seamless traceability of green hydrogen and its derivatives, is being discussed [15].

This paper examines the use of blockchain technology for the traceability of green hydrogen based on the following research questions:

RQ1: What role can blockchain technology play in the hydrogen supply chain?

RQ2: What are the requirements for a proof of origin for hydrogen, and how can a blockchain-based implementation succeed?

2. Background

2.1 Hydrogen Supply Chain

Efforts of the European Union and the Federal Government of Germany to successfully manage the energy transition require the rapid and widespread adaption of existing infrastructure and machinery. The extent of how existing supply chains are affected, can be seen in the example of North Rhine Westphalia, Germanys state with the highest industrial density of steel, chemical and power sites [16]. Only 6.2% of the primary energy consumption of the state has been achieved by sustainable energy sources in 2021 [17]. With an estimated

hydrogen demand of 127-177 TWh by 2045, of which 90% is estimated to be satisfied by imports, challenges in transport, distribution, and storage become apparent [16].

In ambient atmospheric conditions, hydrogen is an ultralight gas with a density of just 0.082 kg/m³ and a high flammability range with air. This results in expensive and complex handling processes to safely move sufficient amounts needed in industrial applications [18]. According to Iulianelli *et al.* [19], 40-75% of the total expenses of the hydrogen supply chain are caused by distributing hydrogen from producer to consumer.

Niermann *et al.* [2] describe an exemplary supply chain for the import of green hydrogen by the following steps, which are visualized in figure 1. First, renewable energy sources, like wind turbines or photovoltaic systems, are utilized to generate electricity. Subsequently, the generated power is transformed into hydrogen using electrolysis. Produced hydrogen is conditioned before export to enable safe and efficient transportation. Rasul *et al.* [18] describe various conditioning approaches, including liquifying and pressurizing hydrogen, or converting hydrogen into derivatives such as ammonium. Conditioning approaches differ by maturity, investment, efficiency, capacity and lifetime, and therefore, must be selected depending on the requirements and nature of the use case. For example, the state of North Rhine Westphalia supports projects like "GET H2", which drive the buildout of hydrogen pipelines to distribute green hydrogen from the Netherlands to local industrial parks. While of substantial investment compared to other conditioning approaches, transportation via pipeline can be worthwhile for lower distances between production and consumption and provides a high maturity level [18]. Other means of transportation than pipelines include ships or trucks. The conditioned hydrogen is stored in reserves such as tanks or caverns within the importing country before it is distributed to the target sites. There, the conditioning process is reversed to reconvert into hydrogen or to achieve the desired physical conditions.

While additional research is needed to discover novel approaches and to further optimize the existing ones, the challenges of the hydrogen supply chain go beyond the safe and efficient transport and storage of hydrogen. According to Ratnakar *et al.* [20], the high cost and lack of existing infrastructure, which is only slowly developed and deployed, hinders the global energy transition. As most hydrogen is currently being produced using fossil fuels, the desired sustainability impact of adopting hydrogen is missed. The authors argue that the high cost and low availability of renewable electricity hinder the widespread adoption of green hydrogen. While additional research is needed to discover novel approaches and to further optimize the existing ones, the challenges of the hydrogen supply chain go beyond the safe and efficient transport and storage of hydrogen. Additionally, efforts of the European Parliament point towards a strong regulation of the production process of green hydrogen [21]. In 2023, the European Union passed the Renewable Energy Directive III, which pushes the disclosure of used energy mixes for the production of hydrogen in an effort to provide standardized guarantees of origin [22].

2.2 Blockchain in hydrogen supply chain

The hydrogen supply chain is characterized by its complexity and multifaceted nature. Blockchain technology is a central enabler for digitizing logistics, trade, and transaction processes in the hydrogen market [15]. Blockchain technology is a decentralized, distributed, tamper-proof, and cooperatively utilized data storage system [23, 24]. In these infrastructures, accounts are not centrally managed by a single entity but maintained

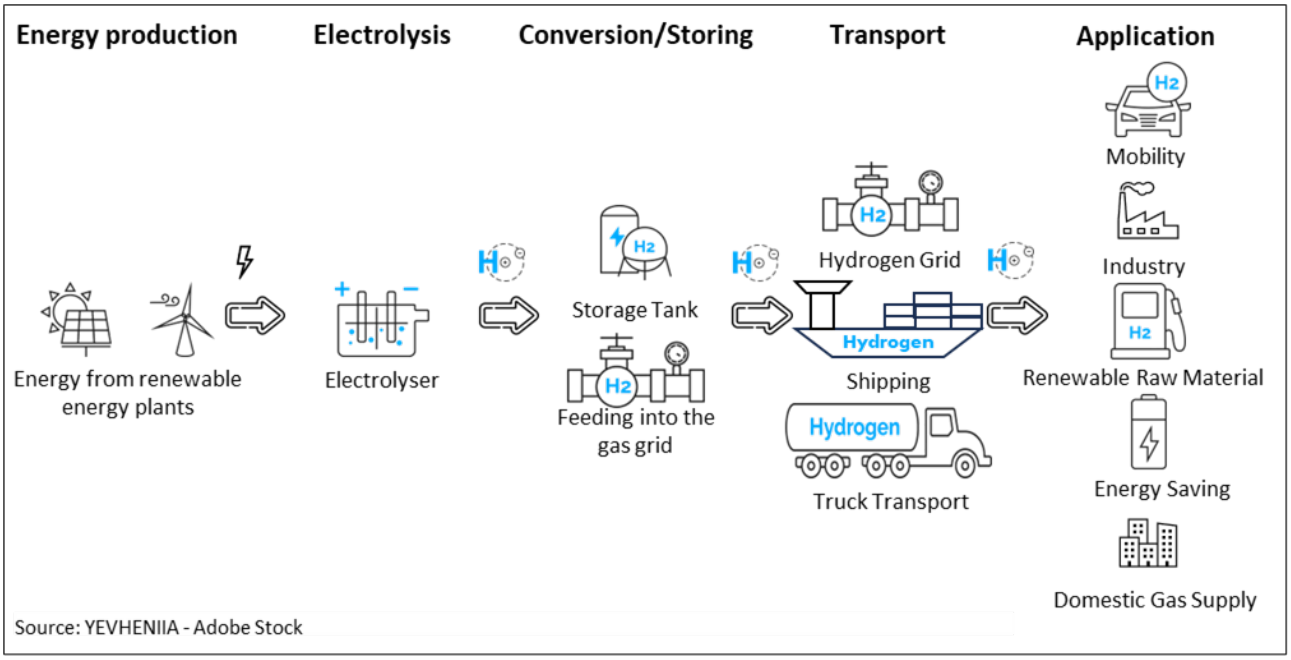

Figure 1: Hydrogen supply chain from energy production to application domain with hydrogen produced by Electrolyser [2]

within a peer-to-peer (P2P) network without a central authority [25]. Blockchain technology employs cryptographic mechanisms to encrypt data sent to the network and stores transactions in "blocks".

Data is distributed among network participants, represented by nodes, which all possess the entire transaction history of a blockchain [23]. A consensus mechanism allows for the validation of transaction contents and decides which node is allowed to form recent transactions into a new block of the blockchain. Once consensus is reached, the new block is added to the existing chain, and the change is broadcast within the network. Each block is linked to the preceding blocks by using hashing algorithms, making it difficult to remove or alter information on the blockchain [26]. Thus, the blockchain is attributed to being tamper-proof and creating a single truth point [27].

Blockchain technology can potentially revolutionize supply chains, especially logistics and inter-company exchange relationships [14]. It connects companies that may not know or trust each other, ensuring transparency, security, and efficiency. Blockchain technology allows companies to manage and synchronize their material, information, and financial flows in a traceable and seamless manner [14, 28, 29], making blockchain particularly suitable for supporting digital value creation in the green hydrogen supply chain.

One promising application of blockchain in the hydrogen economy is certification. The regulatory requirements in Europe stipulate that to produce green hydrogen, either the electricity used must be generated mainly from renewable energy sources or the electricity available in the power grid must be obtained from predominantly renewable energy production [22]. How this process is verified has not yet been conclusively defined. Thanks to its inherent properties, the blockchain promises to automate the necessary certification processes seamlessly from electricity generation to hydrogen production, prove its origin, and bring transparency to the supply chain.

3. Methodology

First, to answer the underlying research questions specified in section 1, a systematic literature review was conducted to examine the present status of hydrogen certification in research. This was added by desk research analysis to further complete the findings with already existing regulatory frameworks regarding the certification of hydrogen in Germany and the European Union. Based on the collected data, a requirements engineering approach was used to derive requirements for a digital solution for certifying renewable hydrogen.

The systematic literature review followed the established guidelines by vom Brocke *et al.* [30] and Webster & Watson [31]. First, the scientific literature database *Scopus* was selected, which was searched in the summer of 2024 using the search term *("proof of origin" OR "Certification" OR "certificate" OR "guarantee of origin") AND "hydrogen."* The literature search was limited to English-language articles published in peer-reviewed journals or conference proceedings. Based on the European hydrogen strategy for a climate-neutral Europe, published in 2020, the period considered for publication was set from 2020 to 2024 [6]. Further, only literature in which the search terms appear in the title, keywords, or abstract was included. This resulted in a selection of 163 articles. Second, the title, keywords and abstract were screened for relevance of content, which led to the selection being reduced to 27 articles. Finally, through a manual full-text screening, which was completed by a forward and backward search, 12 relevant articles were identified.

Additionally, government regulations from the European Union and especially from Germany that are described in the identified literature were added. In this way the regulatory perspective was also included.

The data collection formed the basis for deriving requirements for a digital certification solution for hydrogen. Therefore, according to Pohl and Rupp [32], the requirements engineering approach was used. The method consists of a five-step process model that allows specification and management of requirements. The process is shown in figure 2.

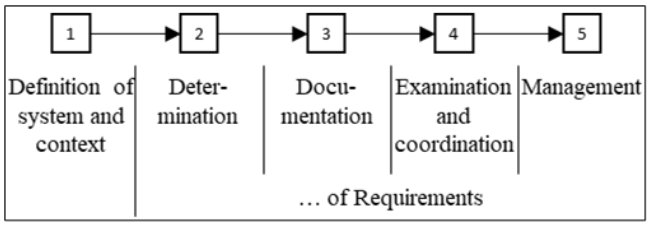

Figure 1: Requirements engineering process according to [32]

First, the system and context were delimited. This paper focuses on the certification of sustainability of hydrogen produced in Germany or transported to Germany through an international or national supply chain. Then, the data from the systematic literature research and the regulatory frameworks were used to determine the requirements. According to Kano *et al.* [33] the derived requirements were divided into basic, performance, and excitement factors. The documentation of the requirements is carried out in section 4. Future scientific work will aim to challenge the identified requirements from the literature and regulatory databases with hydrogen experts. This will also allow the authors to add further requirements derived from expert interviews and workshops. Lastly, the requirements will be translated into design principles, which is the basis for the design process of a blockchain-based solution for the certification of hydrogen.

4. Results

4.1 Requirements for a blockchain-based proof of origin for green hydrogen

In total, 11 requirements were identified from scientific literature and regulatory frameworks. The results were categorized by basis, performance, and excitement factors and are presented in table 1.

Table 1: Derived requirements for green hydrogen certification

Requirement	Source
Basic factors	
Regulatory compliance	[34], [1]
Integrity and accuracy of data	[1], [35]
No double counting	[36], [37], [35]
Consideration of different production pathways	[34], [1], [37]
Transparency	[37], [1], [36]
Performance factors	
Adaptability	[38]
Emission accounting	[34], [39], [40], [41], [38], [13], [37], [42], [37], [43], [35], [44]
International interoperability	[39], [45], [46], [43], [35]
Holistic supply chain integration	[37], [1], [40], [13], [46], [38], [36], [35]
Excitement factors	
Holistic sustainability assessment	[34], [39], [45], [37]
Tradability	[39]

A survey of international energy experts carried out by Goodwin *et al.* [34] revealed that *regulatory compliance* is the criterion most frequently rated as "essential" for a certification solution. This is also confirmed by Abdin [1], who considers this requirement as a basis for technology-based certification solutions. Examples for important regulatory requirements that must be met by German hydrogen players are the European Renewable Energy Directive II (REDII) [43], the European Renewable Energy Directive III (REDIII) [35], and the German Federal Immission Control Act (37. BImSchV) [44].

In the complex networks of hydrogen supply chains, data is exchanged at numerous intersection points. The integrity and accuracy of data must be ensured to operate efficiently and to be able to prove compliance with legal requirements [1]. According to REDIII [35], this also applies to data included in a certification solution. The directive requires that the issued proofs of origin are accurate, reliable and fraud-proof.

Another requirement for the certification solution is to guarantee that emission reductions and the certificate itself are not *double-counted* along the supply chain [36, 37]. This is particularly important for the intersection point between renewable energy and hydrogen certificates [37]. This requirement can also be found according to REDIII [35]. The directive requires that for one unit of sustainable energy only one proof of origin can be created and that every unit of sustainable energy can only be considered once.

In order to allow everyone to assess the sustainability of the hydrogen available to them, *all production pathways* should be certified [37, 34]. This includes the corresponding production inputs and various hydrogen products [34]. As a result, sustainable hydrogen can be clearly distinguished from less sustainable variants [1].

Existing solutions for the certification of hydrogen do not enable end-to-end tracking due to their centralized structures. This results in a lack of *transparency*, which in turn indicates a certain susceptibility to manipulation [1]. Due to the increasing decentralization in the energy market, there is a need for a consistent traceability [36].

To date, there is no standardized classification system that defines when hydrogen is considered sustainable. In particular, the definition by color is not meaningful and implies sustainability, especially via the green color, without providing verified arguments for this [41]. It is therefore necessary to create transparency and comparability by linking the definition to the carbon content of hydrogen [37]. Beyond that, as new hydrogen production processes may be developed in the future certification solutions must be *adaptable* to new conditions [38]. Accordingly, a certification solution should include *emission accounting*. From a regulatory perspective, according to RED II [43] and RED III [35], hydrogen is defined renewable if it is produced by electrolysis based on renewable energy sources. In addition, various constellations and specific requirements like additionality, geographical correlation and temporal correlation are mentioned. However, a specified threshold for carbon content of green hydrogen is still missing. RED II [43] only contains the requirement that hydrogen may be considered renewable if its use leads to a 70 percent reduction in CO_2 emissions. This has already been translated into German law with the 37. BImSchV [44]. An exception is the recently published import strategy of the German Federal Government, which sets the GHG limit at a maximum of 3.4 kg CO_2 eq/kg H_2 [12]. It is not known at the time of publication of this article whether this threshold will be incorporated into a legal provision.

The incompatibility of certificate solutions between import and export countries complicates international trade and hinders the establishment of a global hydrogen market. Therefore, it is necessary to ensure the *international interoperability* of certificates [46]. In addition, different countries have different views on which criteria should be used for the classification and certification of renewable hydrogen. Exporting countries such as Chile or Australia are therefore facing the challenge of having to decide which certification solutions and standards they want to comply with [41]. On the other hand, countries relying on hydrogen imports, such as Germany, will

need to decide which approaches they accept [39]. For both cases, an international harmonization would greatly reduce friction of hydrogen trade. From a regulatory perspective RED II and RED III can be seen as attempts to harmonize the European hydrogen market [43, 35].

The example of blue hydrogen shows that emission accounting is applied very differently from case to case [37]. Accordingly, for a standardized certification, it is necessary to integrate the whole supply chain (*holistic supply chain integration*) from electricity generation to end-user consumption [1, 13]. This also means that hydrogen-based products like green steel must be included in the certification solution [38]. Furthermore, the intersection points has to be defined, so that the transfer of information is regulated between the different supply chain participants [37]. However, the RED III announces a database for tracking of liquid and gaseous renewable fuels and recycled carbon-containing fuels. Here, among others, information about the lifecycle carbon emissions of hydrogen that occur from the place of production to the moment the hydrogen is used or traded in the European Union will be saved [43].

In addition to the carbon emissions that occur along the hydrogen supply chain, further environmental and social aspects have to be considered [37]. For example, the electrolysis process has a high demand for water, which can negatively impact water resources, especially in water-stressed regions [34]. Therefore, a *holistic sustainability assessment* is necessary for certification.

According to Steinbach & Bunk [39], who investigated a suitable hydrogen market design by conducting interviews in five expert groups, most experts prefer a system that allows for the *tradability* of the certificates.

4.2 Blockchain for hydrogen certification

The use of blockchain and certificates is still relatively new in the energy industry and their synergies are not investigated sufficiently to date [36, 47]. Research in the field of blockchain focuses primarily on its use in financial and general supply chain management applications, while the fields of application in hydrogen networks are hardly considered [48]. To help close this research gap, this section explains how blockchain-based solutions can contribute to fulfill the identified requirements for certifying the sustainability of hydrogen. The explanations are based on the previously shown example of a supply chain for hydrogen produced by an electrolysis process (figure 1).

Starting with energy generation, it can be observed that the electricity grid is becoming increasingly digitized. This is accompanied by the challenge of guaranteeing data security [36]. By capitalizing on increasing digitization, blockchain offers a solution for data security challenges, as data manipulations become known to the network through the cryptographic processes and hash functions of blockchain [49]. Additionally, the energy market is becoming increasingly decentralized due to the spread of renewable energy plants [50]. In such an environment, the technology can provide traceability of data on renewable energies by distributing transparent information between the different actors in the energy market [50, 36]. The collection, network-wide distribution and tamper-proof storage of data are rendering blockchain to be a suitable approach for proof of origin or certification cases. A general framework for a blockchain-based certification process is described by Wannack [15]. The author suggests that energy trading between an electricity producer and the electrolysis operator can take place by tokenizing the amount of electricity produced, storing the tokens on a blockchain and transfer them as proof of origins.

At the second stage of the hydrogen supply chain, sustainable energy is used by electrolysis operators to produce green hydrogen. According to Ferraro *et al.* [13] the blockchain offers the potential to convert the available electricity data into proof of origins for hydrogen automatically using smart contracts. Data on the plant model and the performance of the electrolyzer are taken into account for this purpose. In addition, smart contracts can be used to measure "the quantity of carbon dioxide avoided in relation to the quantity of hydrogen produced" ([13], p.5).

The proof of origin is passed on along the subsequent stages of the hydrogen supply chain, including conversion, transport, storage and consumption. In these stages the risk of data misuse is minimized by the tamper-proof architecture of the blockchain, creating trust between the supply chain actors. To tackle the oracle problem, further security mechanisms can be installed on the data-recording devices [9]. A blockchain-based solution can therefore assure the sustainability of the hydrogen.

Another challenge in supply chains which influences a certification solution is the unwillingness of actors to share data [51, 52]. According to Heeß [9], this can be solved by adding other confidence-building components such as identity management to the blockchain solution. Therefore, concerns regarding data protection can be counteracted by reducing the public disclosure of data. In addition according to Mould *et al.* [36], it is also noted that a blockchain-based solution has the potential to be accepted as an international standard due to its inherent advantages such as transparency and trust. This would solve the problems of the today's fragmented landscape of certification solutions and facilitate the cross-border trade of hydrogen.

In summary, blockchain-based solutions can replace conventional centralized certification solutions that do not offer consistent transparency. The decentralized architecture of a blockchain offers the potential to track every stage of a hydrogen supply chain and thus enable end-to-end certification for hydrogen from electricity production to the end consumer [1]. The proof of origins

can be created automatically using smart contracts according to defined rules and passed on along the supply chain [13]. Moreover, the data stored on the blockchain is characterized by transparency and integrity, which makes the certification process secure and traceable [1].

5. Outlook

In this article, 11 requirements were derived from the literature and regulatory frameworks. These are shown in table 1. Despite the still rather low level of research on the certification of the sustainability of hydrogen, it is evident that there is already a broad consensus in research, particularly regarding the requirements for emissions accounting, holistic supply chain integration and a holistic sustainability assessment. However, conventional certification solutions are reaching their limits regarding the identified requirements for hydrogen certification. Innovative digital solutions are therefore needed, with blockchain proving to be particularly promising. Thanks to its inherent properties, it offers the potential for consistent end-to-end certification along the entire hydrogen supply chain. In addition, the data stored on the blockchain is characterized by transparency and tamper-proofness, which can result in a high level of trust in the solution. This brings the vision of an internationally standardized certification solution that facilitates cross-border trade within reach.

To date, the synergies between blockchain solutions and the certification of hydrogen have not been sufficiently investigated. This work represents a systematic contribution to closing this research gap. To this end, the existing literature and regulatory frameworks were first examined for requirements for hydrogen certification and then derived how the blockchain as the underlying technology of a solution can contribute to solving the requirements.

Building on this, further research work will aim to validate and supplement the identified requirements through interviews with practice partners. The requirements are then translated into design principles for a blockchain-based solution, which is the basis for the development of a practice-oriented solution. This procedure is already implemented in the research project described below.

Acknowledgments

This work is funded by the Ministry of Economic Affairs, Industry, Climate Action, and Energy of the State of North Rhine-Westphalia under the funding code "EFRE-20200044" from funds of the EFRE/JTF program.

To explore the potential of blockchain technology in the hydrogen economy, a blockchain-based certification system for green hydrogen is being researched as part of the "DUH-IT" project. In this project, requirements for blockchain-based proof of origin are being gathered, focusing on developing and validating prototypes within a test network. The project seeks to create a reliable solution that ensures seamless traceability of green hydrogen, thereby enhancing transparency and security in the hydrogen supply chain. By utilizing blockchain technology, the system aims to prevent manipulation and ensure data integrity. The overarching goal is to develop innovative solutions that promote a sustainable hydrogen economy.

Contact details

Tobias Wappner:
tobias.wappner@iml.fraunhofer.de

Alexander Grünewald:
alexander.gruenewald@iml.fraunhofer.de
ORCID: 0000-0003-2983-348X

Maik Hausmann:
maik.hausmann@iml.fraunhofer.de

References

[1] Z. Abdin, “Empowering the hydrogen economy: The transformative potential of blockchain technology,” *Renewable and Sustainable Energy Reviews*, vol. 200, p. 114572, 2024.

[2] M. Niermann, S. Timmerberg, S. Drünert, and M. Kaltschmitt, “Liquid Organic Hydrogen Carriers and alternatives for international transport of renewable hydrogen,” *Renewable and Sustainable Energy Reviews,* pp. 1–15, 2021.

[3] Bundesregierung, *Anteil der Erneuerbaren Energien steigt. Fragen und Antworten zur Energiewende,* https://www.bundesregierung.de/breg-de/schwerpunkte/klimaschutz/faq-energiewende-2067498#:~:text=Deutschland%20soll%20bis%202045%20klimaneutral,mehr%20Tempo%20bei%20der%20Energiewende., 2024.

[4] J. E. G. Baquero and D. B. Monsalve, “A Proposal for the Transformation of Fossil Fuel Energy Economies to Hydrogen Economies Through Social Entrepreneurship,” in *Entrepreneurial Innovation for Securing Long-Term Growth in a Short-Term Economy.* P. Ordóñez de Pablos, J. Gamez-Gutierrez, J. M. Saiz-Alvarez, Eds.: IGI Global, 2021, pp. 48–70.

[5] H. Ishaq, I. Dincer, and C. Crawford, "A review on hydrogen production and utilization: Challenges and opportunities," *International Journal of Hydrogen Energy*, vol. 47, pp. 26238–26264, 2022.
[6] European Commission, "A hydrogen strategy for a climate-neutral Europe," *COM,* pp. 1–23, 2020.
[7] L. Gawlik and E. Mokrzycki, "Analysis of the Polish Hydrogen Strategy in the Context of the EU's Strategic Documents on Hydrogen," *Energies*, vol. 14, p. 6382, 2021.
[8] N. de Blasio and C. Hua, "The Role of Blockchain in Green Hydrogen Value Chains," *Policy Brief,,* pp. 1–4, 2021.
[9] P. Heeß, J. Rockstuhl, M.-F. Körner, and J. Strüker, "Enhancing trust in global supply chains: Conceptualizing Digital Product Passports for a low-carbon hydrogen market," *Electron Markets*, vol. 34, pp. 1–20, 2024.
[10] J. Moya, I. Tsiropoulos, D. Tarvydas, and W. Nijs, *Hydrogen use in EU decarbonisation scenarios,* https://jointresearch-centre.ec.europa.eu/system/files/2019-04/final_insights_into_hydrogen_use_public_version.pdf, 2019.
[11] T. Smolinka, Wiebe Nikolai, P. Sterchele, A. Palzer, F. Lehner, and M. Jansen, et al., *Studie IndWDe. Industrialisierung der Wasserelektrolyse in Deutschland: Chancen und Herausforderungen für nachhaltigen Wasserstoff für Verkehr, Strom und Wärme,* 2018.
[12] *Importstrategie für Wasserstoff und Wasserstoffderivate,* 2024.
[13] M. Ferraro, P. Gallo, M. G. Ippolito, F. Massaro, E. R. Sanseverino, and S. Ruffino, et al., "A test bench for the production of green hydrogen and its traceability and certification using blockchain technology," in *2023 IEEE International Conference on Environment and Electrical Engineering and 2023 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe):* IEEE, 2023, pp. 1–6.
[14] A. Grünewald, T. Gürpinar, C. Culotta, and A. Guderian, "Archetypes of blockchain-based business models in enterprise networks," *Inf Syst E-Bus Manage,* 2024.
[15] V. Wannack, "Blockchain Based Hydrogen Market (BBH2) - A Paradigm-Shifting, Innovative Solution for a Climate-Friendly and Sustainable Structural Change," *Open Conf Proc*, vol. 2, pp. 59–63, 2022.
[16] MWIKE NRW, *Wasserstoff Importkonzept Nordrhein-Westfalen,* https://www.klimaschutz.nrw.de/fileadmin/Dateien/Download-Dokumente/Broschueren/240725_Wasserstoff_Importkonzept_NRW.pdf, 2024.
[17] Landesbetrieb IT.NRW, *NRW: Anteil erneuerbarer Energieträger am Primärenergieverbrauch 2021 um 1,9 Prozent gesunken. Der Primärenergieverbrauch insgesamt stieg dagegen um 5,0 Prozent gegenüber dem Vorjahr an. Der Anteil erneuerbarer Energieträger daran ist auf 6,2 Prozent gesunken.,* May, 2024.
[18] M. G. Rasul, M. Hazrat, M. A. Sattar, M. I. Jahirul, and M. J. Shearer, "The future of hydrogen: Challenges on production, storage and applications," *Energy Conversion and Management*, vol. 272, p. 116326, 2022.
[19] A. Iulianelli, F. Dalena, and A. Basile, "H2 production from bioalcohols and biomethane steam reforming in membrane reactors," in *Bioenergy Systems for the Future. H2 production from bioalcohols and biomethane steam reforming in membrane reactors.* Elsevier, Ed., 2017, pp. 321–344.
[20] R. R. Ratnakar, N. Gupta, K. Zhang, C. van Doorne, J. Fesmire, and B. Dindoruk, et al., "Hydrogen supply chain and challenges in large-scale LH2 storage and transportation," *International Journal of Hydrogen Energy*, vol. 46, pp. 24149–24168, 2021.
[21] E. Gregor and Svensson Sara, "EU rules for renewable hydrogen," *Members´ Research Service,* 2023.
[22] European Union, *Directive (EU) 2023/2413 of the European Parliament and of the Council of 18 October 2023 amending Directive (EU) 2018/2001, Regulation (EU) 2018/1999 and Directive 98/70/EC as regards the promotion of energy from renewable sources, and repealing Council Directive (EU) 2015/652,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023L2413&qid=1699364355105, 2023.
[23] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain Technology in Business and Information Systems Research," *Bus Inf Syst Eng*, vol. 59, pp. 381–384, 2017.
[24] N. Große, D. Leisen, T. Gürpinar, R. S. Forsthövel, M. Henke, and M. ten Hompel, *Evaluation of (De-)Centralized IT technologies in the fields of Cyber-Physical Production Systems.* Hannover : publish-Ing, 2020.
[25] V. Morabito, *Business innovation through blockchain. The B3 perspective.* Cham. Springer, 2017.
[26] S. Nakamoto, *Bitcoin: a peer-to-peer electronic cash system,* 2008.
[27] N. Große, T. Guerpinar, and M. Henke, "Blockchain-Enabled Trust in Intercompany Networks Applying the Agency Theory," in *2021 3rd Blockchain and Internet of Things Conference.* New York, NY, USA: ACM, 2021, pp. 8–14.

[28] V. Wannack, “Blockchain Technology as a Catalyst for a Sustainable and Efficient Green Hydrogen Supply Chain,” in *Proceedings of the Future Technologies Conference (FTC) 2023, Volume 3*, vol. 815. K. Arai, Ed. Cham: Springer Nature Switzerland, 2023, pp. 367–372.
[29] M. S. Hernandez, I. Sentosa, F. Gaudreault, I. Davison, and F. H. Sharin, “The Emergence Of The Metaverse In The Digital Blockchain Economy: Applying The Esg Framework For A Sustainable Future,” in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE):* IEEE, 2023, pp. 1324–1329.
[30] J. vom Brocke, A. Simons, B. Niehaves, K. Reimer, R. Plattfaut, and A. Cleven, “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process,” *ECIS 2009 Proceedings,* pp. 2206–2217, 2009.
[31] J. Webster and R. T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS Quarterly: Management Information Systems*, vol. 26, pp. xiii–xxiii, 2002.
[32] K. Pohl and C. Rupp, *Basiswissen requirements engineering: Aus- und Weiterbildung zum“Certified Professional for Requirements Engineering”. foundation level nach IREB-Standard.* dpunkt.verlag, 2015.
[33] N. Kano, N. Seraku, F. Takahashi, and S. Tsuji, “Attractive quality and must-be quality,” *Journal of the Japanese Society for Quality Control*, vol. 14, pp. 39–48, 2.
[34] D. Goodwin, F. Gale, H. Lovell, K. Beasy, H. Murphy, and M. Schoen, “Sustainability certification for renewable hydrogen: An international survey of energy professionals,” *Energy Policy*, vol. 192, p. 114231, 2024.
[35] European Commission, *Directive (EU) 2023/2413 of the European Parliament and of the Council of 18 October 2023 amending Directive (EU) 2018/2001, Regulation (EU) 2018/1999 and Directive 98/70/EC as regards the promotion of energy from renewable sources, and repealing Council Directive (EU) 2015/652. REDIII.* EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023L2413&qid=1699364355105, 2023.
[36] K. Mould, F. Silva, S. F. Knott, and B. O’Regan, “A comparative analysis of biogas and hydrogen, and the impact of the certificates and blockchain new paradigms,” *International Journal of Hydrogen Energy*, vol. 47, pp. 39303–39318, 2022.
[37] M. Riemer, “Lessons learnt from certifying biofuels for a future hydrogen certification scheme,” in *2022 18th International Conference on the European Energy Market (EEM):* IEEE, 2022, pp. 1–7.
[38] P. Majewski, F. Salehi, and K. Xing, “Green hydrogen,” *AIMSE*, vol. 11, pp. 878–895, 2023.
[39] S. A. Steinbach and N. Bunk, “The future European hydrogen market: Market design and policy recommendations to support market development and commodity trading,” *International Journal of Hydrogen Energy*, vol. 70, pp. 29–38, 2024.
[40] M. H. A. Khan, T. Sitaraman, N. Haque, G. Leslie, S. Saydam, and R. Daiyan, et al., “Strategies for life cycle impact reduction of green hydrogen production – Influence of electrolyser value chain design,” *International Journal of Hydrogen Energy*, vol. 62, pp. 769–782, 2024.
[41] J. Chandler and J. Paterson, “Selling sunshine: Emerging challenges in the certification of hydrogen,” *Journal of Energy & Natural Resources Law,* pp. 1–19, 2024.
[42] A. Velazquez Abad and P. E. Dodds, “Green hydrogen characterisation initiatives: Definitions, standards, guarantees of origin, and challenges,” *Energy Policy*, vol. 138, p. 111300, 2020.
[43] European Commission, *Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast) (Text with EEA relevance.). REDII.* EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.328.01.0082.01.ENG&toc=OJ:L:2018:328:TOC, 2018.
[44] Bundesministerium der Justiz, *Verordnung zur Neufassung der Siebenunddreißigsten Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes 1, 2 (Verordnung zur Anrechnung von strombasierten Kraftstoffen und mitverarbeiteten biogenen Ölen auf die Treibhausgasquote),* https://www.gesetze-im-internet.de/bimschv_37_2024/, 2023.
[45] F. Gale, D. Goodwin, H. Lovell, H. Murphy-Gregory, K. Beasy, and M. Schoen, “Renewable hydrogen standards, certifications, and labels: A state-of-the-art review from a sustainability systems governance perspective,” *International Journal of Hydrogen Energy*, vol. 59, pp. 654–667, 2024.
[46] L. V. White, R. Fazeli, W. Cheng, E. Aisbett, F. J. Beck, and K. G. Baldwin, et al., “Towards emissions certification systems for international trade in hydrogen: The policy challenge of defining boundaries for emissions accounting,” *Energy*, vol. 215, p. 119139, 2021.
[47] P. O’Donovan and D. T. J. O’Sullivan, “A Systematic Analysis of Real-World Energy Blockchain Initiatives,” *Future Internet*, vol. 11, p. 174, 2019.
[48] J. Li, M. S. Herdem, J. Nathwani, and J. Z. Wen, “Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management,” *Energy and AI*, vol. 11, p. 100208, 2023.
[49] P. de Filippi, M. Mannan, and W. Reijers, “Blockchain as a confidence machine: The problem of trust & challenges of governance,” *Technology in Society*, vol. 62, p. 101284, 2020.

[50] A. Ahl, M. Yarime, M. Goto, S. S. Chopra, N. M. Kumar, and K. Tanaka, et al., “Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan,” *Renewable and Sustainable Energy Reviews*, vol. 117, p. 109488, 2020.
[51] K. Berger, J.-P. Schöggl, and R. J. Baumgartner, “Digital battery passports to enable circular and sustainable value chains: Conceptualization and use cases,” *Journal of Cleaner Production*, vol. 353, p. 131492, 2022.
[52] W. Liu, X.-F. Shao, C.-H. Wu, and P. Qiao, “A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development,” *Journal of Cleaner Production*, vol. 298, p. 126763, 2021.

Role-based Smart Contract Programming for Factory-in-a-Box

Orçun Oruç, Uwe Aßmann
TU Dresden, Software Technology, Dresden, Deutschland

Over the past few decades, meeting customer demands has evolved due to extended delivery times, expensive manufacturing skills, and a need for flexibility. Competitive technologies have created gaps among manufacturers, impacting their ability to meet customer expectations. A major issue is the visibility of production capabilities and loads within the supply chain network. The "Factory-in-a-Box" concept addresses this by moving machinery between locations. Reconfigurable manufacturing systems provide benefits like reduced management time, versatile products, and lower costs. Successful implementation requires reliable transfer of hardware and software configurations. However, planning machinery transfers can be unreliable, necessitating accurate reconstruction at the new site. We propose using role-based smart contracts to ensure machinery reconfigurability in a "Factory-in-a-Box" system. These smart contracts can uphold the preconditions and postconditions for equipment concerning new software configurations. This study presents qualitative and quantitative analyses, summarizing the findings.

Keywords: Blockchain-based Manufacturing Technology, Smart Contracts, Role-based Programming Language

1. Introduction

1.1 The research problem

Classical production systems have traditionally operated within a static supply chain network located in a specific region. However, in response to changes in the manufacturing system requirements, dynamic production transfer system called "Factory-in-a-Box" have emerged. Factories need to be set up at new production sites rapidly. To this end, hardware components should efficiently be integrated with software components. Furthermore, when multiple customers require specific manufacturing devices from different factories, a common and shareable database should provide information about peak production time, allocated production capacity, and the possible procurable amount of production devices from a given factory.

Manufacturing strategy decision is an important phase of the decision in factory-in-a-box realization. It depends on facility (location, size, focus), capacity (amount, acquisition time), and process technology (flexibility, type of equipment, technology level) [1]. These strategy decisions can change the requirement of situations in various locations. The Factory-in-a-Box concept has been analyzed planning level, hardware level that integrates production modules into mobile platforms [2]

Smart manufacturing technologies are emerging as important technological focal points that integrate customer information and data with production systems [3]. Data from information systems should be verified for ownership records, identity information, security configurations, and transactions between machineries. For instance, additive manufacturing (3D printing) can be useful for customization, rapid prototyping, and promptly making spare parts [4]. When implementing such a system that encompasses all of the aforementioned requirements, requirements data should be verifiable at each requirements, data should be verifiable at each requirement with timestamp value, hash value in business transactions at each operation, source and destination addresses of method invocation, and confirmation numbers regarding the business transaction. Smart contracts provide consensus with cryptography on data integrity solutions in private data pools, unlike end-to-end communication encryption.

The Factory-in-a-Box comprises standardized production modules that can be installed on a transportation medium such as a truck or plane to make transportation easier [5]. Manufacturing machineries undergo states during the assembly of the tool components. In the present day, the sustainable reconfigurability of Factory-in-a-Box is a crucial concept, aiming to provide rapid and non-intrusive methods for transferring machineries between customer locations without extensive efforts. To achieve this goal, one can explore the advantages of software systems that assist in configuring manufacturing for existing machinery in a factory as well as security of Factory-in-a-Box system. Ordering a "Factory-in-a Box" can help entrepreneurs reduce costs and save time by implementing a project within a limited timeframe. For instance, one can outsource a production environment globally. However, a challenge lies in determining the availability of the outsourcing production environment. Another issue arises with the transportation of the production environment to the customer's premises. To complete this process, the production line from outsourced company should be finalized.

Moving production systems from industrialized countries to low-income countries can be facilitated by smart contract technology, as well as between industrialized

countries. This is because internal and external requirements of machinery configuration are confirmed through historical data within a smart contract. Given the distance between countries, rapid deployment and the validity of software configuration becomes more crucial than regional deployment of a production company. However, the same gap can be found between industrialized countries. For instance, skilled workers might be a deficit points for a particular industrialized country that needs to be addressed. One solution could be for a production company in an industrialized country to fill the skillset gap through Factory-in-a-Box transfer, with rapid role-based configuration of smart contracts. Security and safety in production systems are also equally important for production companies.

After a natural event or disruptive events occurs, customers may consider transferring existing manufacturing devices along with damaged environment and configuration data. However, completing this task is challenging without a software system, and it becomes even more difficult when using a traditional software system, such as centralized client-server applications. For instance, auditing of the configuration and setup data for production machinery in a centralized software system can be challenging in the aftermath of a disruptive event, as the system itself may be damaged or compromised.

Smart contract security and tamper-proof validation of manufacturing software are major outcomes. While manufacturing systems focus on production rate, quality delivery, and profit to match robust software systems perfectly. There is regular routine between layers in manufacturing systems and the interaction between these layers is directly linked to cost factors that can increase or decrease cost inflation in production systems [6]. According to Bengtsson et al. [7], mobility and speed, which comprise condition monitoring, outsourcing of complete maintenance, condition monitoring for unscheduled stops and troubleshooting are key elements of Factory-in-a-Box [7].

Software configuration changes have a tremendous effect on machinery devices in the manufacturing industry. The primary goal of the software configuration is to provide plug-and-play components that can load the existing modules of Factory-in-a-Box and embed the information layer autonomously (in a verification chain) into Factory-in-a-Box without requiring extensive human intervention. Changing parameters of Factory-in-a- Box can affect the Overall Equipment Efficiency (OEE) in the runtime of machinery of Factory-in- a-Box; however, one can compare the efficiency and availability of the entire system with this parameter as we have discussed the details of OEE in subsection 7.4.

In Chapter 5, a motivational use case with three different modules is defined: *ProductionController*, *RoleAssigner*, and *ProductionConfigurator*. The main purpose of the use case outlined in Methodology 5 is to demonstrate the feasibility of role modeling and smart contract-based Factory in a Box, with testable parameters discussed in Result 7. While *RoleAssigner* is associated with role modeling, *ProductionConfigurator* and *ProductionController* are related to Factory-in-a-Box machinery control.

2. Motivation and Challenges

The main motivation is to showcase state-of-the art decentralized software solution (smart contracts) for Factory-in-a-Box concept. Factory-in-a-Box concept, which is anticipated to play a crucial role for future manufacturing outsourcing. Determining trust in outsourcing is a pivotal factor for deciding which companies can be deemed credible. For example, each step of a production should be traceable in historical data when necessary. There is also a concern that Factory-in-a-Box machineries could be used for illegal activities or harmful development. To mitigate such risks, the use of smart contracts might be beneficial. From this perspective, establishing credibility and ensuring information flow security between participants are essential points.

To highlight our motivations, we pose two different research questions as follows:

• **Research Question 1 (RQ1):** Research Question 1 (RQ1):

Are the current smart contract programming technologies suitable for facilitating the transfer of machinery in the context of a Factory-in-a-Box?

• **Research Question 2 (RQ2):**

How can we leverage the trust and auditing features of smart contracts in a manufacturing transfer system?

We will evaluate the findings related to these research questions in Chapter 10.

3. Outline of Objectives

In this study, we aim to present a case study on Factory-in-a-Box outsourced manufacturing. In doing so, we will outline objectives of the task and our contributions in the following statements. The areas we will cover include manufacturing technology, concepts for the strategic development of automation, and tools for the intelligent reuse of experience, knowledge, and information.

The objectives of this study can be listed as follows:

• Define the requirements of software features for transferring manufacturing and rapid prototyping with respect to an outsourced production module.
• Provide a smart contract-based solution with role-based assignment for rapid deployment and mobility of flexible production capacity.
• Specify parameters regarding the mobile pro- duction unit configuration to work with smart contracts.
• Analyze drawbacks and advantages associated with decentralized smart contract development methodologies.

4. Related Work

Winroth and Jackson et al. have proposed a fundamental theory bridging the gap between traditional manufacturing strategy and mobilization of the production environment **[1]**. A manufacturing strategy can affect multiple divisions of a company such as marketing, research and development, and accounting. According to authors, factory in a box concept should have the following key concepts:

• **Flexibility:** Different joint preparations with short set-up time are necessary to have flexible equipment and fixtures.

• **Mobility:** A production platform should be moved anywhere and it can be dispatched to a supplier or to a on-site manufacturing company.

• **Speed:** Quick reconfiguration of a production module is vital for outsourcing so that one can ensure the right level of automation by decreasing the disturbance time.

Angrish et al. **[8]** have carried out a prototypical implementation that consists of fabrication service providers with a couple of nodes which are simulating a mining process with a Turing complete language. In order to save the cost of energy from the consensus algorithm in manufacturing domain, the authors utilized Proof of Authority. In the end, they have built up a system that comprises of the flow of assets with metadata in shareable database that can incentivize the participation of various manufacturer stakeholder on a network.

Pasha et al. **[9]** (Pasha et al. 2020) propose the vehicle routing algorithm regarding factory in a box concept that involves assembling factories in containers and transporting the containers to different customer locations. The proposed algorithm decides whether there is a high demand over a given time period in an area or not. If there is a high demand, a production location can be temporarily stationed and deployed near customers.

Ask and Stillström et al. have defined to use factory- in-a-box concept in several areas, which as follows [10]:

• Mobile manufacturing systems should provide reconfiguration ability and efficient knowledge of the system infrastructure.

• Mobile manufacturing systems can collaborate on production capacity with other companies.

• Mobile manufacturing systems can handle occasional peaks in production.

• Mobile manufacturing systems should provide reconfiguration ability and efficient knowledge of the system infrastructure.

Mobile manufacturing systems can be installed in a decentralized manner.

• Mobile manufacturing systems may address temporary disturbances in a supply chain.

• Mobile manufacturing systems should maintain shareable leasing contracts for production capacity.

The authors of the paper have defined key performance indicators as mobility, flexibility, and speed in the Factory-in-a-Box concept. The process should be quick and flexible, observing in different phases of configuration, transportation, installation and ramp-up. Moreover, the authors claim that factors such as equipment, competence, and manufacturing process have a significant impact on the machinery configuration.

Olsson et al. [5] claim that an increasing interest in production capacity or modules should be configured in a short time without extensive in house expertise and enabled increased capacity. Experience transfer is an invaluable asset for a fast, flexible and mobile configuration of a Factory-in-a-Box production module. This can reduce operation cost for on-site companies.

4.1 Role-Modeling of Smart Contracts

Role modeling involves the multiple identification of an object in order to abstract it at a higher level and create context-specific view [11]. The Decorator pattern is well-known pattern used to dynamically add supplementary responsibilities to an object [12]. Roles can be represented in different ways in object-oriented programming methodology, such as through mixins, traits, subtyping by multiple inheritance, and interface separators in smart contracts. The functional requirements of roles have been mentioned by Kuhn [13] , and Steimann [14]. In these research studies, they have defined roles features, including role relationships, simultaneous role playing, abandonment and acquirement of roles dynamically, deep roles, and access restriction of roles, comprising over 20 features in detail. However, our research aims to focus on features that are not covered in most of the role-based studies. On the contrary, we define role-based features as constants through smart contract library definitions in a simplistic way.

Role objects are embodied by core objects that can be instances of a specific class. Similar to subtyping from a class, a role can be assigned through inheritance from a superclass. However, in certain programming languages, inheritance must be linearized, as they do not support multiple inheritance due to the diamond problem. In this study, we simplified this process to demonstrate the straightforward assignment of identities to machinery members, such as *MaintenanceAgent*, *Production Controller*, *Production Configurator* and *RobotArm* in our case study.

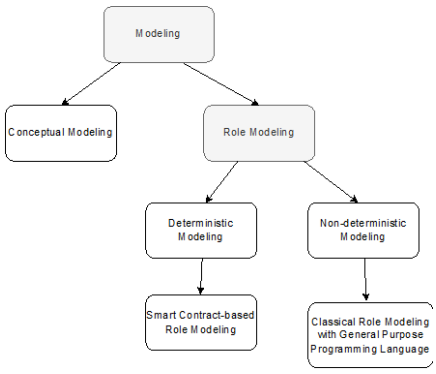

Figure 1: Concept of the Smart Contract Modeling

As illustrated in Figure 1, roles can be de- fined in both non-deterministic and deterministic ways across different programming languages. A role encompasses properties, behaviors, and states. Roles are often specified as contextual, representing various states of an object within different contexts. Contextual roles aid in adapting to diverse situations or environments through both deterministic and non-deterministic modeling. Non-deterministic role modeling does not maintain a consistent state of attributes and methods when adapting to dynamic environments. In order to check context of roles, one can use library constants to validate role identity within a context at runtime.

5. Role-Modeling of Smart Contracts

In this chapter, we will model the case study solution with deterministic smart contract modeling. We present a case study applicable to in a manufacturing company that needs to lease production capacity or outsource production. As illustrated in Figure 1, the role model underlying smart contract is deterministic, implying that the same attributes of roles will consistently generate the same hash in the programmable ledger.

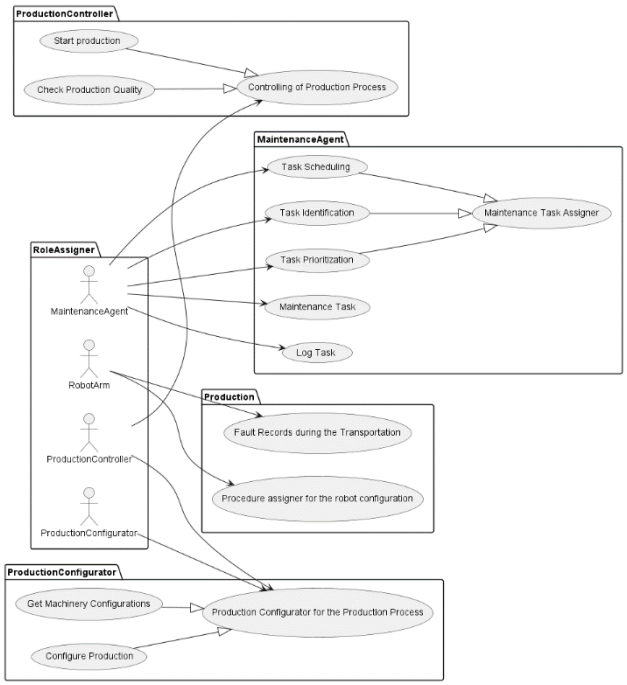

Figure 2: Case Study Diagram for Factory-in-a-Box Machinery Transfer

In Figure 2, we have role assigner and maintenance agent modules as main modules and pro- duction controller, production configurator, and production modules as supplementary modules.

As shown in Figure 3, the authors will follow the described methodology with respect to the research study. In terms of the methodology, the research on Role-based Smart Contract Programming for Factory-in-a-Box begins with defining the research problem and demonstrating the results. We have two fundamental research questions, RQ1 and RQ2. After defining the research questions, result demonstration is planned concerning the method of demonstration in the results section, along with relevant limitations regarding the results. With the help of a metamodel diagram of smart contracts for Factory-in-a-Box featuring role modeling, one can easily follow the details of the design patterns, such as the mediator pattern, chain of responsibility pattern, and constant-based role assignment. The feasibility of the design patterns for role modeling should be evaluated with a use case in the implementation.

6. Implementation of the Case Study

6.1 Constant-based Role Modeling for Factory-in-a-Box and Conceptual Modeling

In order to design the Decentralized Factory-in- a-Box solution, we have used metamodeling approach with sequence and class diagrams.

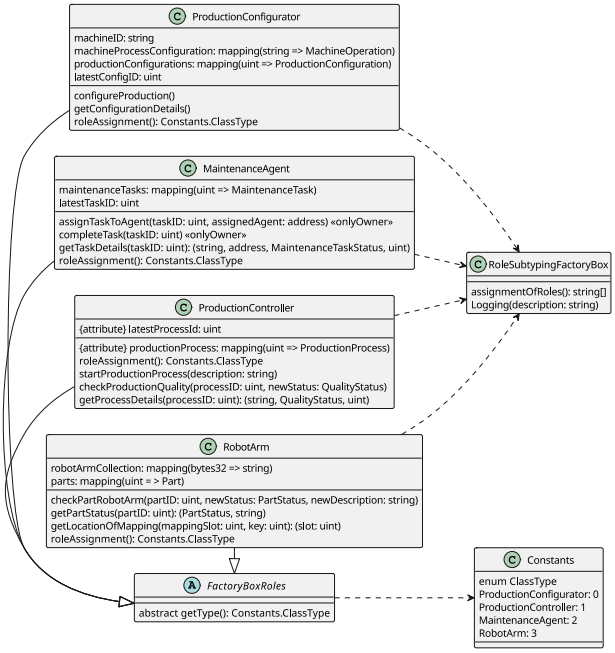

Figure 3: Class Diagram of the Main Modules of the Case Study

check validity of the production status after trans- ferring the machinery. *ProductionConfigurator* set machine configuration details during transfer process and configure the environment robot arm (machinery) and a specific process in the production module. *MaintenanceAgent* smart contract ensures all maintenance task can be achieved by *MaintenanceAgent* role in three different statuses which are open for maintenance, in progress maintenance, and completed for the maintenance.

In order to show details of the smart contract- based Factory-in-a-box system, we need to list our requirements regarding the case study in Figure 2. The general case study in Figure 2 will be defined different smart contracts and each of them can be thought as modules. *MaintenanceAgent*, *ProductionConfigurator*, *ProductionController*, and *RobotArm* are multiple modules that control a machinery transfer process. Machineries are assembled from different parts that can be produced by manufacturers or services. Roles should be assigned to different parts of the Factory-in-a-Box system through

smart contracts to make consistent identities between factory-in- a-box role members.

The *ProductionConfigurator* can configure the production environment with machinery using a configuration ID and a specific role name. Roles are defined by smart contract constants in a smart contract library, which is one of the smooth ways to abstract smart contract objects to obtain a role- based identity. The Role subtyping smart contract (*FactoryBoxRoles*) can interact with different types of roles such as maintenance agent, production configurator, production controller, and robot arm. Lastly, the robot arm can interact with roles in order to complete certain tasks related to the production configurator and production controller. The metamodel diagram can be depicted in Figure 4. In this metamodeling, we have main roles that can be created by subtyping from super smart contract (FactoryBoxRoles) of Factory-in-a-Box System.

Each constant is recorded into a library to govern subtyping with smart contracts. Smart contract should validate the right constant whether it is used for a role type or not. The drawback of this approach is to create overhead code size. As shown in code snippet 1, we have defined four different smart contract roles, which are *MaintenanceAgent*, *ProductionController*, *ProductionConfigurator* and *RobotArm*, in a single contract that has been used for subtyping property.

A robot arm can manage different states of production steps in code snippet 1. These steps have been influenced by the study of Mpofu et al. [15]. Basically, these are the fundamental movements for a robot arm of CNC Milling 1. As shown in Code Snippet 1, the *roleAssignment()* function is defined as virtual function of a smart contract. Solidity is the highly enhanced object-oriented smart contract language that allow us to utilize abstraction, encapsulation, overloading, composition, association, and polymorphism. When a business transaction occurred, a sample data structure can be appeared as follows:

As depicted in Algorithm 1, we can summarize business transaction hash algorithm in smart con- tract programming. The cost of system transfer can be defined by the cost of transactions in smart contracts. For instance, if one calls *setupMachinery()* method multiple times, the cost of the state variable, method invocation, and contract deployment will be calculated accordingly. Transactions are stored in a Merkle Hash Tree and in case of a change in the next transaction, hash tree data structure will be altered.

Algorithm 1: Transaction validity with hash algorithm

Data: Transaction List:
$H(A) \rightarrow H(B) \rightarrow H(C) \rightarrow H(D)$
Result: $H(A|B|C|D)$
Data: x: input function, d: data of the transaction, H: hash
Result: transaction(x) = H(d)

Algorithm:;
begin
$transaction(x) \leftarrow \text{hash}(d)$;
$H(A|B) \leftarrow H(A) + H(B)$;
$H(C|D) \leftarrow H(C) + H(D)$;
$H(A|B|C|D) \leftarrow H(A|B) + H(C|D)$;
return $H(A|B|C|D)$;
end

6.2 Mediator Pattern for Role Assignment

Mediator pattern is used to assign hierarchy to child objects from a parent object. The objective of roles in Mediator pattern is to map on parent role and the role of child roles [16]. The coordination between child objects and parent objects are controlled by a mediator object. Mediator object manages roles, providing dynamic binding of core and role objects.

As can be seen in Figure 5, the Mediator pattern can be implemented for role assignment as a different module in Factory-in-a-Box systems. *Mediator* and *ConcreteMediator* in the system provide a communication mechanism between roles. *RobotArmRole* and *ProductionControlRole* are sample roles that associate with *ConcreteMediator* and *RoleImplementor*.

7. Result

We will analyze the result aspect of qualitative and quantitative results which will have performance parameters, deployment costs, and usage of the system for quantitative analysis. Qualitative analysis answers research questions and flexibility of smart contracts' usage.

Execution speed of the Factory-in-a-Box system can be a parameter. In order to provide short execution process between locations, short set-up time for machineries in Factory-in-a-Box transfer is essential. All modules should be verified within a reasonable amount of time and this phase should be transparent.

Another criteria could be the speed of role assignment in different design pattern implementation. Which one is quicker for the validation phase. However, speed of a smart contract can rely on the complexity of a smart contract. A smart contract complexity can be calculated by gas cost as shown in the Table 1.

7.1 Quantitative Analysis

Roles	Deployment Cost
RobotArm	510822 gas
MaintenanceAgent	771008 gas
ProductionConfigurator	574042 gas
ProductionController	684901 gas
UpdatedRobotArmV1	1015819 gas
UpdatedRobotArmV2	1021383 gas
OEECalculator	236206 gas
Role Methods	**Execution Cost**
completeTask	36287 gas
logMaintenanceTask	119357 gas
configureProduction	136696 gas
startProductionProcess	116519 gas
assignTaskToAgent	53771 gas

Table 1: Deployment and Execution Cost of Smart Contracts

The following Table 1 shows the main methods of *RobotArm*, *ProductionConfigurator*, *ProductionController*, *UpdateMaintenance V1 and V2* to demonstrate execution cost of corresponding smart contracts. Updated version of a contract through Universal Upgradable Proxy Standard (UUPS) contract does not change the size of contract dramatically. Although the assignment of role contracts take half of the crypto-cost, proxy contract for role method update for robot arm can be cost-efficient way for smart contract programming. As depicted in Table 1, execution costs of a set of methods are higher than deployment costs. Execution cost depends on the complexity of business logic in a method.

Parameters include the performance of the smart contract execution, deployment costs, and execution costs in terms of spending of cryptocurrency. Deployment cost of a smart contract or a group of smart contracts as estimated amount in a cryptocurrency. This cost can also indicate the complexity analysis of a smart contract, as a simpler codebase of a smart contract results in lower smart contract deployment fees for developers. In our Factory-in-a-Box system, we have different members of factory-of-a-box system, *MaintenanceAgent*, *ProductionConfigurator*, *ProductionController*, and *RobotArm*. For role-based assignments, we use *FactoryBoxRoles* with constant types across various smart contracts.

Deployment and execution costs are show in Table When observing the charts of deployment and execution cost, the line of text on the left-hand side shows the relevant information of the cost. The upper side of the left-hand side text demonstrates the second types of cost. For instance, as illustrated Figure 8, under the line of deployment cost, it demonstrates the deployment cost of the design pattern. The upper line of the left-hand side shows the execution cost of the design pattern. This should be considered while evaluating the final result.

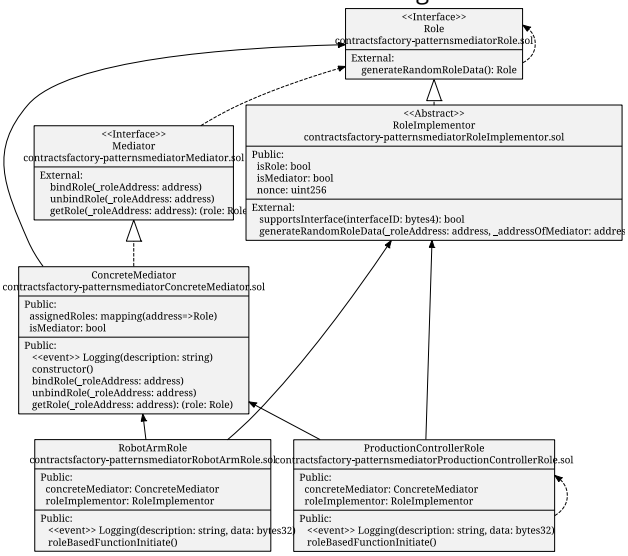

Figure 5: Mediator Design Pattern for the Role Assignment in Factory-in-a-Box

7.2 Qualitative Analysis

The research questions have already been defined as RQ 1 and RQ 2. Current smart contract techniques, particularly in terms of domain-specific programming languages, are not always suitable for complex applications. Solidity, chosen as one of the enhanced smart contract languages for this study, faces challenges due to its lack of input/output systems and multithreading capabilities, especially for real-time data analysis from multi-node applications in the Factory-in-a-Box context. While achieving a small-scale application for software configuration validation is possible with an object-oriented smart contract programming language, Ethereum (Solidity) may not be ideal for high transaction speeds in a blockchain network due to considerations of cryptocurrency cost and speed.

7.3 Validation Tests for Factory-in-a-Box Smart Contracts

We plan to implement the following parameters in order to provide scientific results for validation tests.
• **Input Parameters:** This test includes aspects of boundary values, edge cases, and invalid inputs to verify that the contract handles them correctly. They can be tested with unit tests in smart contracts.
• **State Changes:** Verification that the smart contract correctly updates its state according to the specified logic and conditions.
• **Event Emission:** Testing the emission of events by the smart contracts to ensure that relevant events are emitted when certain conditions are met. Events are valuable for logging and monitoring the health of the Factory-in-a-Box system. Each smart contract triggers an event during its execution cycle.

• **Gas Usage**: Measurement and evaluation of the gas consumption of a smart contract to ensure efficient operation in use cases of Factory-in- a-Box.

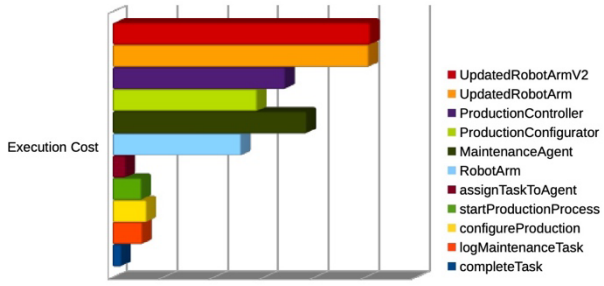

Figure 6: Role Deployment with Role Constants and Execution Cost Chart

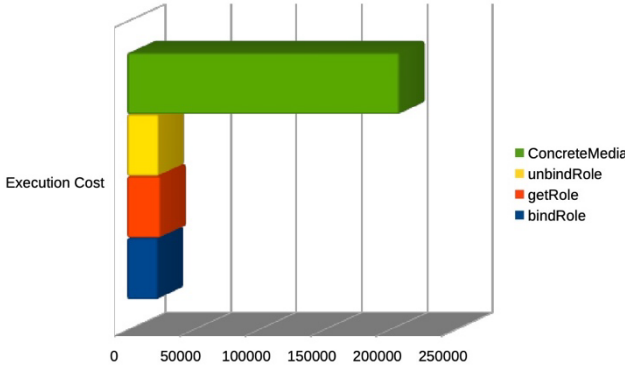

Figure 7: Role Deployment with Mediator Pattern Execution and Deployment Cost

Mediator Pattern Role Deployment	Deployment Cos
ConcreteMediator	208274 gas
Mediator Pattern Role Methods	**Execution Cost**
bindRole()	23425 gas
getRole()	25601 gas
unbindRole()	24107 gas

Table 2: Deployment and Execution Costs of Mediator Pattern Role Deployment

7.4 Overall Equipment Efficiency Calculation for Factory-in-a-Box

Overall Equipment Efficiency (OEE) is a combined metrics with Availability, Performance and Quality that can show us a transported factory unit efficiency after installation phase. While running entire machineries of a factory, to calculate OEE is important for monitoring and evaluation phases. Availability, Performance, and Quality can be calculated with remarks called Operating Time (OT), Ideal Cycle Time (ICT) and Total Count (TC) as follows:

$$\text{Performance} = \frac{\text{OT} \times \text{ICT} \times \text{TC}}{100} \quad (1)$$

$$\text{Quality} = \frac{\text{Good Units}}{\text{Total Units Produced}} \times 100\%$$

$$\text{Availability} = \frac{\text{Scheduled Production Time}}{\text{Operating Time}} \times 100\%$$

Finally, we can infer the last calculation which is relevant to the OEE to assess the performance of equipment or machinery.

$$\text{OEE} = \text{Availability} \times \text{Performance} \times \text{Quality}$$

This equation utilizes input parameters to com- pare results before the implementation of the Factory-in-a-Box solution and after its implementation. This allows for runtime monitoring and validation of the end-to-end process. Availability indicates the percentage of time that equipment is available for production during scheduled time. Performance defines how close the equipment operation can converge to its maximum theoretical speed. Quality refers to the ratio of good-quality output to the total output, taking into account defects and rework. You can assess OEE parameters with smart contracts.

7.5 Observations from the use case

During the definition of use case regarding Factory- in-a-Box, the following observations have been made:

• Design pattern selection is important for the speed of validation with regards to machinery transfer and configuration. Design pattern line mediator, observer, chain of responsibility, and role-object model have own definition and drawbacks in the practical use.

• Role modeling should be tailored according to a specific requirement of the use case.

• Role modeling can limit the system functionality in case of alteration of requirements because the underlying design pattern should be tailored.

• If the ecosystem of the use case grows, de- sign pattern selection of role-based assignment choice should be change because the system can affect the selection of design pattern underlying role concept. The complex implementation of the design pattern, the more consumes crypto asset in the underlying system, which can cause the high asset costs in main Ethereum networks.

• The cost of transaction and speed between com- ponents are dependent on the type of networks as well as the way of implementing the entire system.

8. Limitations

The following limitations should be considered when evaluating the results of this research paper:
• The evaluation of the paper is conducted in test networks. The result of the gas cost can vary in real blockchain networks depending on sidechains.
• Role assignment with metamodeling is the main focus of Factory-in-a-Box in this use case.
The use case scenarios have been limited to a single case, as shown in Figure 2.
• The results section is evaluated based on gas limit, complexity of the use case application, overall equipment analysis, and ablation studies.
• The context of the paper is limited to Factory- in-a-Box machinery transportation and the cal- culation of machinery efficiency, as well as the result of machinery after transportation from one location to another.

9. Discussions

In order to understand the validation of this re- search, we can focus on three different points: accuracy, reliability, and generalizability of the proposed solution whether or not it causes to compromise for manufacturing technology with regards to Factory-in-a-Box. Accuracy can be measured by cryptoasset spending for its ability to execute the programming logic properly. Most of time, validity of Factory-in-a-Box system can be considered as the validity of smart contract transaction. If the smart contract transaction has a stall in the network or logical errors, validity of the system can be endangered. Transaction can be converted into an algorithm as follows:
Transactions, as illustrated Figure in 1, are stored in a Merkle tree to constitute chain of blocks in a blockchain network. Every method invocation with state variables are registered into a transaction and a transaction can validate the Factory-in-a-Box system.
As for the sensitive analysis, by conducting sensitivity analysis, smart contract developers can gain valuable insights into how different parameters affect the contract's behavior and performance. This information can inform design decisions, identify potential risks and vulnerabilities, and ultimately lead to the development of more robust and effective smart contracts.
OEE parameter could be a testing parameter for end-to-end system integration in Factory-in-a-Box. Modules can be tested internally and external final result aspect of transportation in Factory-in-a-Box can be possible to calculate with OEE formula 7.5.

This can reduce the operation costs, reconfiguration time and validation of reconfiguration of Factory-in-a-Box machineries.
Validation of this research paper can be considered through the validation test parameters outlined in Section 7.3. For example, gas usage is a crucial parameter for validating the Overall Equipment Efficiency (OEE) Calculation formula during the runtime of software components. State changes can be validated based on alterations in the state, which is closely related to gas costs. Type casting can be utilized to validate the cor- rectness of the role-based deployment module, ensuring proper role subtyping. Furthermore, smart contracts are deterministic software applications, meaning that the state of smart contracts with data layers can be protected during runtime. Smart con- tract applications designed for Factory-in-a-Box should produce the same number of transactions and hashed blocks under the same inputs, serving as a major validation step for Factory-in-a-Box.

10. Conclusion

The main purpose of this paper is to introduce a new approach to assembling configuration of production models in containers and delivering software configuration through role-based smart contract members for rapid deployment. In essence, our study proposes a basic version of machine transfer capability in terms of Factory-in-a-Box technology. We have inferenced the following findings from the implementation chapter.

The findings can be found as follows:

The Factory-in-a-Box solution can be implemented with object oriented smart contract programming languages.
• Smart contracts can ensure the traceability of production configuration and establish post- and preconditions of software configuration on the customer site.
• Production Configurator can be traced with smart contracts' transactions. Traces can be recorded to logging data structure (emit-event data structure of Solidity).
• Upgrading smart contract for new features cost less than the deployment of a new contract without proxy contract. Roles can be updated through proxy contracts without spending high amount of cryptocurrency(gas). According to this finding, new role creation and upgrading will have a doubled-size cost without proxy contract upgrading.

The implementation of case study code can be found at the following link1.

10.1 Paper Contributions

A state-of-art design, analysis and implementation with regard to smart contract development with Factory-in-a-box concept.
• Practical analysis of the Factory-in-a-Box concept within a containerized trusted and auditable environment.
• Implementation of Factory-in-a-Box by means of the smart contract programming.

[1] https://github.com/zointblackbriar/PaperCode/tree/main/ Factory-in-a-Box

• Configuration of compactness and portability of manufacturing devices for rapid deployment and validation of runtime and setup configuration.
• Comparison for role-based identity assignment for Factory-in-a-Box to demonstrate extended implementation cases for future usage. Comparison of role-based identity assignment qualitatively and quantitatively.
The following contributions have been analysed between subchapters.

11. Future Work

Smart contracts can be implemented with different technologies to meet specific requirements of the Factory-in-a-Box concept. For instance, if high transaction speed is essential in a blockchain net- work, Algorand smart contracts may handle this. Smart contracts can be implemented with different technologies to meet specific requirements of the Factory-in-a-Box concept. For instance, if high transaction speed is essential in a blockchain network, Algorand smart contracts may handle this better and faster than Ethereum contracts 5. An analysis of various consensus algorithms can be conducted for decentralized machinery transportation, such as Proof of History (Solana Blockchain) , Proof of Stake (Ouroboros-Cardano), or Delegated Proof of Stake (Cosmos).

Acknowledgement

This work is funded by the German Research (DFG) within the Research Training Group Role-Based Software Infrastructures for continuous-context-sensitive Systems (GRK 1907).

Bibliography

[1] J. M. Winroth M., „Manufacturing competition through the Factory-in-a-Box concept," *In: Proceedings of the 18th Annual POM Conference ,* 2007.
[2] J. M. F. P. S. J. S. R. C. J. B. M. W.-r. M. Hedelind M., „Factory-in-a-Box–Solutions for availability and mobility of flexible production capacity," *In: Proceedings of SPS Vol. 7, pp. 28–30,* 2007.
[3] D. L. S. A. N. F. Frank A. G., „Industry 4.0 technologies: Implementation patterns in manufacturing companies.," *International journal of production economics 210, pp. 15–26,* 2019.
[4] B. D. B. R. Phuyal S., „Challenges, Opportunities and Future Directions of Smart Manufacturing: A State of Art Review," *In: Sustainable Futures 2, p. 100023 https:// www.sciencedirect.com/science/article/pii/S2666188820300162,* 2020.
[5] H. M. A. M. U. F. P. Olsson E., „Experience reuse between mobile production modules-an enabler for the factory-in-a-box concept.," *In: The Swedish Pro-duction Symposium. Gothenburg, Sweden,* 2007.
[6] P. J., „Concept of a manufacturing system," *In: International Journal of Pro-duction Research 17(2), pp. 123–135 https://doi.org/10. 1080/00207547908919600,* 1979.
[7] E. S. J. M. Bengtsson M., „The factory-in-a-box concept and its maintenance application.," *In: Kumar U., Parida A., Rao R. (eds.) Proceedings of the 19th Congress of Condition Monitoring and Diagnostic Engineering Manage- ment (COMADEM). Luleå, Sweden,* 2006.
[8] C. B. H. M. S. B. Angrish A., „A Case Study for Blockchain in Manu-facturing: "FabRec": A Prototype for Peer-to-Peer Network of Manufacturing Nodes.," *In: Procedia Manufacturing 26, pp. 1180–1192 https://www.sciencedirect.com/science/article/pii/S2351978918308308,* 2018.
[9] D. M. A. K. M. A.-o. O. F. W. H. G. W. Pasha J., „An Optimization Model and Solution Algorithms for the Vehicle Routing Problem With a "Factory-in-a-Box".," *In: IEEE Access 8, pp. 134743–134763,* 2020.
[10] S. C. Ask A., „Mobile Manufacturing Systems: Market Requirements and Opportunities.. Mälardalen University, Department of Innovation, Design and Product Development. http://www.ijme.us/cd_06/PDF/IT%20301- 014.pdf," 2006.
[11] R. D. S. W. W. M. Bäumer D., „The role object pattern.," *In: Proceedings of PLoP, pp. 97–34,* 1997.
[12] G. E., „Design patterns," *Pearson Education India He C., Nie Z., Li B., Cao L., He K. (2006) Rava: Designing a Java ,* 1995.
[13] K. T., A family of role-based languages, 2017.
[14] S. F., „On the representation of roles in object-oriented and conceptual modelling.," *In: Data & Knowledge Engineering 35(1), pp. 83–106,* 2000.
[15] T. N. Mpofu K., „Multi-level decision making in reconfigurable machining systems using fuzzy logic," *In: Journal of Manufacturing Systems 31(2), pp. 103–112,* 2012.
[16] R. D., „Composite design patterns," *Proceedings of the 12th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications ,* p. pp. 218–228, 1997.

A framework for selecting and integrating blockchain devices into supply chain management

Tan Gürpinar [1], Thuy Tien Nguyen Thi [2], Maximilian Austerjost [2]
[1] Quinnipiac University, Hamden, USA
[2] Fraunhofer IML, Dortmund, Germany

With blockchain technology revolutionizing data exchange and process automation, companies face challenges in securely transferring data, connecting devices, and facilitating ecosystem interactions. We outline a three-phase methodology for selecting and integrating blockchain devices, focusing on their application in supply chain management: (1) initial use case classification, (2) comparison with existing blockchain devices and (3) taxonomy-based fine-tuning. This structured approach combines technology selection procedures with the device taxonomy to provide actionable guidance. Key findings include the selection criteria of blockchain devices, a detailed classification of current devices, and practical recommendations for their application in supply chains. The framework emphasizes blockchain's potential to enhance transparency, security, and efficiency in logistical processes, offering valuable insights for both companies and blockchain enthusiasts.

1. Introduction

Blockchain technology is revolutionizing various industries by offering enhanced security, transparency, and efficiency in data management and process automation. This technological advancement is particularly relevant in supply chain management, where the need for secure and transparent data exchange is critical. However, an empirical study on the adoption of blockchain technology among German companies revealed that only 12% have implemented it in their supply chains so far [1]. Despite its potential, one of the primary challenges is that blockchains, by default, cannot access real-world off-chain data. This limitation significantly constrains the scope of blockchain applications, particularly in supply chains [2]. Therefore, blockchain devices, which facilitate the connection between physical assets and digital records, play a crucial role in leveraging the benefits of blockchain technology in real-world applications.

The importance of researching blockchain devices stems from the fundamental principle that the effectiveness of a blockchain system is heavily dependent on the quality and integrity of the data it processes [3]. Inadequate or erroneous data inputs can lead to unreliable outputs, undermining the system's credibility and effectiveness. Hence, the precise selection and integration of blockchain devices are paramount to ensuring that data remains accurate, consistent, and trustworthy throughout the supply chain [4].

Despite the growing adoption of blockchain technology, there is a notable lack of comprehensive frameworks for selecting and integrating blockchain devices [5]. Current research often focuses on theoretical aspects of blockchain technology or general technology selection methods, which do not adequately address the unique requirements and challenges associated with blockchain devices [6, 7]. This gap in the literature highlights the need for a specialized methodology that addresses both the technical and practical aspects of blockchain device integration.

This paper seeks to address this gap by exploring how companies can systematically select and integrate blockchain devices to enhance their operational efficiency and data integrity. The research question guiding this study is:

How can organizations effectively choose and implement blockchain devices to maximize their operational benefits and ensure reliable data processing?

The paper is structured to first present a definition of the most relevant terms and a detailed methodology for the selection and integration of blockchain devices. It will then analyze the characteristics and capabilities of existing devices, followed by a discussion of practical implementation strategies. Finally, the paper will provide recommendations for future research and development in this area, aiming to support organizations in achieving optimal performance and reliability in their blockchain systems.

2. Theoretical Background

Blockchain devices are pivotal in ensuring the effectiveness and reliability of blockchain systems by serving as the interface between physical assets and digital ledgers. These devices capture and transmit real-world data into the blockchain, making them essential for maintaining the integrity and accuracy of the information recorded on the blockchain. The theoretical background for blockchain devices revolves around several core concepts and challenges:

Data Integrity and Accuracy: Blockchain systems rely on the principle of data immutability, where once data is recorded on the blockchain, it cannot be altered without detection. However, the accuracy of this data is contingent upon the quality of the input provided by blockchain devices. If a device transmits erroneous or

tampered data, it can compromise the integrity of the entire blockchain ledger. Research in this area focuses on developing technologies and methodologies to ensure that data captured by blockchain devices is accurate, reliable, and resistant to tampering.

Device Security: Given that blockchain devices act as the entry point for data into the blockchain, they must adhere to stringent security protocols to prevent unauthorized access and data breaches. This includes implementing robust encryption methods, secure communication channels, and anti-tampering mechanisms. Theoretical frameworks in this domain explore best practices for securing these devices against various types of cyber threats and vulnerabilities.

Integration and Compatibility: Blockchain devices need to seamlessly integrate with existing infrastructure and blockchain networks. This involves addressing challenges related to interoperability, standardization, and compatibility with other systems and devices. Research in technology integration theory examines how blockchain devices can be effectively incorporated into current processes, ensuring that they operate harmoniously within the broader technological ecosystem.

Performance and Scalability: The performance of blockchain devices is crucial for the overall efficiency of blockchain systems. This includes factors such as processing speed, data transmission rates, and the ability to handle large volumes of data. Theoretical research in this area investigates how to optimize device performance to support scalable blockchain applications and prevent bottlenecks in data processing and communication.

Human-Device Interaction: The usability of blockchain devices impacts their effectiveness and adoption. This aspect covers the design of user interfaces, ease of operation, and the ability of devices to provide actionable insights. Research in human-device interaction focuses on improving user experience, which is vital for ensuring that blockchain devices are practical and user-friendly for their intended applications.

By addressing these theoretical aspects, research on blockchain devices can advance our understanding of their role in enhancing the functionality and reliability of blockchain systems. This background provides a basis for developing guidelines and best practices for selecting and integrating blockchain devices, ensuring that they contribute positively to the overall performance and security of blockchain applications.

3. Methodology

The methodology for researching blockchain devices involves a systematic approach to examining their characteristics, performance, and integration into blockchain systems. This approach includes a combination of qualitative and quantitative methods to ensure a comprehensive analysis. The following steps outline the methodology:

Literature Review: We start with a review of existing literature on blockchain devices, focusing on their roles, functionalities, and the challenges associated with their implementation. This step involves analyzing academic papers, industry reports, and case studies to build a foundational understanding of the current state of blockchain device technology and identifying gaps in the research.

Device Classification: We then collect information on the method and the criteria that is used to classify the devices as well as their functions and applications. This classification includes sensors, IoT devices, hardware wallets, and other peripherals that interact with blockchain systems. To classify the devices in a first step (Device Matrix in Chapter 4), we follow the methods developed by [8, 9, 10], which focus on selecting technologies by setting future goals and working backward from there. This approach, known as "retropolation," helps to identify pathways towards achieving these goals. It involves techniques like experience curves, S-curve analyses, and scenario planning.

Among these, the portfolio technique is particularly useful for choosing technologies that need to be implemented within a timeframe of up to 5 years. Therefore, we based our method on the portfolio analysis by [11]. Building on this, this article introduces a portfolio analysis specifically suitable for blockchain devices and uses it for its initial classification process. In a second step, the classification is refined by describing the requirements for the device starting from the information obtained from the matrix of the previous step. For this refinement, the article utilizes a multidimensional taxonomy as described by [12] as this tool has already been successfully utilized to classify blockchain supply chain use cases [13] and hardware [3]. Following the method, in this article a morphological box is used to describe the blockchain device based on predefined dimensions. The taxonomy is used to describe the device required for the use case in a more granular way by selecting appropriate characteristic values for each dimension. The aim is to enable users to draw detailed conclusions and formulate their own requirements for the device.

Case Studies and Interviews: We conduct case studies and interviews with industry experts, developers, and users of blockchain devices to validate theoretical findings and gather practical insights. The former provides practical examples of how devices are used in real-world scenarios, while interviews offer qualitative insights into user experiences, challenges faced, and best practices.

Data Collection and Analysis: We gather quantitative data through surveys, experiments, or testing protocols. This data may include device performance metrics, security assessments, and user feedback. Analyze this data using statistical methods to identify patterns, correlations, and trends. This analysis provides empirical evidence to support the research findings and conclusions.

Comparative Analysis: We perform a comparative analysis of different blockchain devices based on the established criteria. This involves evaluating the strengths and weaknesses of each device category, as well as their suitability for various applications. The comparative analysis helps to identify the most effective and reliable devices for specific use cases.

Integration Strategies: We develop and evaluate strategies for integrating blockchain devices into existing systems. This includes assessing compatibility with different blockchain platforms, identifying integration challenges, and proposing solutions. The aim is to provide practical guidelines for seamless integration and optimal performance.

Recommendations and Best Practices: Based on the findings, we formulate recommendations and best practices for selecting, implementing, and managing blockchain devices. These recommendations are designed to guide stakeholders in making informed decisions and improving the overall effectiveness of blockchain systems.

By following this methodology, the research aims to provide a comprehensive understanding of blockchain devices, their functionalities, and their impact on blockchain systems. The approach combines theoretical insights with practical evidence to offer valuable guidance for researchers, practitioners, and developers in the field.

4. Blockchain Device Matrix

In the following, four blockchain devices are explained as examples and to give a better understanding of how such devices are used in a supply chain scenario:

Temp2Net: This is an IoT device designed for monitoring temperature-sensitive goods along supply chains. It integrates blockchain technology to document and secure data such as location and internal temperature. The device includes a high-resolution e-paper display for real-time information and utilizes a combination of sensors, a light client, and blockchain integration through the Tendermint framework and Cosmos SDK.

DragonDevice: A mobile device developed for handling dangerous goods, DragonDevice focuses on automating and digitizing transport documentation. It supports the carrier by providing electronic transport documents, tracking dangerous goods, and ensuring compliance with regulations. The device features a display, camera, and sensors, and integrates blockchain technology to secure and update transport records. It also supports the "bring your own device" concept to leverage existing mobile hardware.

DragonPuck: This modular IoT device is used for tracking hazardous materials during transportation. It monitors environmental conditions such as temperature, humidity, and acceleration. The DragonPuck operates on energy-efficient batteries, uses Wi-Fi and mobile networks for communication, and integrates with blockchain for transaction recording and data security. The device is designed for long-term operation with minimal maintenance.

Blockchain IoT Gateway: They represent high-performance devices (e.g. a server) that receive data inputs from sensors and send them to a blockchain network. This is necessary as some IoT devices are restricted by their computational performance and memory and therefore cannot participate in blockchain consensus as it is computationally heavy [14].

The following table provides an overview of the two dimensions to create a portfolio analysis of blockchain devices.

Table 1: Features and Examples of Blockchain Devices

Category	Feature	Examples
Mobility	Stationary Device	Server
	Mobile Devices	Tablet, Sensor
Equipment	Low Energy Device	DragonPuck
	Middle Class Device	Temp2Net
	High Performance Devices	DragonDevice

1) Mobility comprises the spatial/local flexibility of the physical blockchain device in the sense of its being (un)bound to a specific location, by describing the transportability or concrete mobility as well as the cable connection. The more pronounced these characteristics are, the higher the mobility of the device can be classified. Two sub-dimensions exist.

Stationary Devices are used in a fixed position (e.g. permanently installed), as no movement is possible or desired on the part of the process (e.g. blockchain gateway server).

Mobile Devices have increasing degrees of freedom for spatial movement, for example because they are moved in the process (e.g. integration on pallets) or there are requirements for the device's own mobility (e.g. tablet, sensors)

2) Equipment characterizes the device in terms of its inherent peripherals and external constitution on the one hand and includes the dimensions of application and communication performance on the other. The higher the identified value of this characteristic, the higher the requirements for the scope of features and performance of the device are assumed. The three-way division into low energy, middle class and high performance devices is based on a classification scheme proposed by the Internet Engineering Taskforce (see Table 2). There, resource-constrained IoT devices are categorized based on their random-access memory (RAM) and flash memory [15].

Table 2: Classification Scheme [based on 15]

Class	Equivalent	RAM	Flash
Class 0	Low Energy	<< 10 kB	<< 100 kB
Class 1	Middle Class	~ 10 kB	~ 100 kB
Class 2	High Performance	~ 50 kB	~ 250 kB

Low Energy Devices allow little or no user interaction and are only used to collect or transmit data. Low-energy devices are also characterized by their low energy consumption, but they generally have limited memory and computing resources (e.g. sensors such as the DragonPuck)

Middle Class Devices are used to support business processes and can be interactively used. They have a number of input, output and operating options. Even though they are more energy-intensive, they have better energy reserves (e.g. rechargeable batteries). Thanks to the memory and computing resources provided, they can perform some tasks themselves in order to control energy requirements, but the device and its functionalities are not used continuously (e.g. Temp2Net).

High Performance Devices have additional peripherals and distinct interaction options, whereby the entire hardware package is more extensive. The high-performance devices are correspondingly energy-intensive, but also offer more comprehensive data processing and data transfer options (e.g. DragonDevice).

After presenting the evaluation criteria for our portfolio analysis, the exemplary devices and other blockchain devices can finally be classified. The (necessary) degree of mobility is shown on the abscissa of the matrix. The ordinate describes the (necessary) performance of the device. Based on these categories, a portfolio diagram is drawn, which can be used to visually classify devices based on the dimensions previously described. There are nine fields within the portfolio matrix, each of which represents a combination of degree of mobility, equipment and performance. According to a simple nearest-neighbor approach, the blockchain devices that are close to the classification of one's own use case in the matrix are suitable as a first approximation (see Figure 1). The smaller the distance between the points, the greater the agreement in the characteristics of the devices.

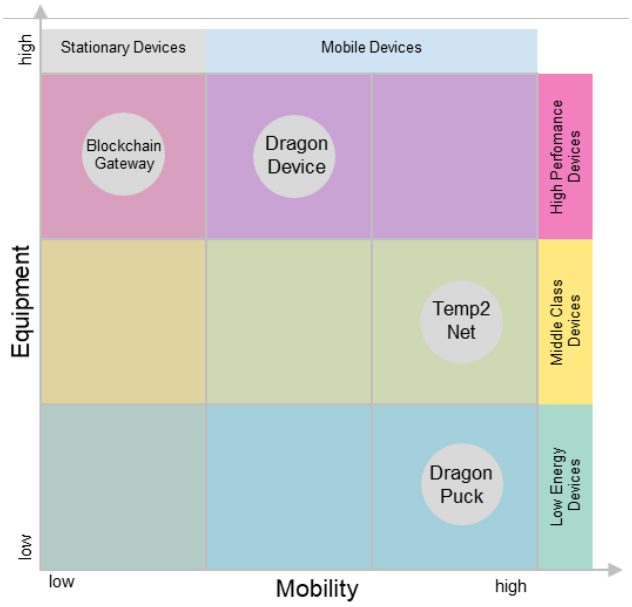

Fig. 1: Blockchain Device Matrix

5. Blockchain Device Taxonomy

In the previous section, we provided a broad classification of blockchain devices, introducing various types and their core functionalities. Here, we delve into a more detailed taxonomy to offer a nuanced understanding of blockchain devices and facilitate further research into their categorization and application.

I. Device Type

a. IoT Devices: These devices are designed for integration into Internet of Things (IoT) ecosystems, enabling real-time data collection and interaction with blockchain networks. They are often equipped with sensors and connectivity features to monitor environmental conditions or track assets. Examples include temperature monitors for supply chains and environmental sensors for hazardous material handling.

b. Mobile Devices: Mobile blockchain devices include smartphones or tablets that have been adapted to handle blockchain transactions or provide specialized blockchain services. These devices often include applications or software for managing digital assets, verifying transactions, or interacting with decentralized applications.

c. Specialized Devices: These are devices tailored for specific use cases or industries, such as compliance documentation for dangerous goods or modular tracking units for logistical operations. They often combine blockchain functionality with industry-specific requirements.

II. Integration Level

a. Full Nodes: Devices operating as full nodes maintain a complete copy of the blockchain and participate in validating and propagating transactions. They typically require significant computational resources and storage capacity.

b. Light Nodes: Light nodes, also known as thin clients, rely on full nodes for blockchain data and focus on reducing computational and storage demands. These devices are often used in environments where resource constraints are a concern, such as mobile or embedded systems.

c. Hybrid Nodes: These devices operate with a mix of full and light node capabilities, balancing between local data processing and reliance on external blockchain networks. They are designed to optimize performance and resource use for specific applications.

III. Application Domain

a. Supply Chain Management: Devices in this category focus on tracking goods through various stages of the supply chain. They may include temperature sensors, GPS trackers, and compliance monitoring tools, all integrated with blockchain for data security and traceability.

b. Environmental Monitoring: These devices are used to measure and report environmental conditions such as temperature, humidity, or air quality. They are crucial in applications where data integrity and real-time monitoring are essential, often used in conjunction with blockchain to ensure data accuracy and reliability.

c. Compliance and Documentation: Devices designed for regulatory compliance and documentation tasks fall into this domain. They often provide functionalities for digital record-keeping, transaction verification, and adherence to legal requirements, leveraging blockchain to secure and verify documents.

IV. Taxonomy

This taxonomy provides a structured framework for classifying blockchain devices based on their type, integration level, and application domain. It serves as a foundation for further research and development, enabling a deeper understanding of how these devices operate and interact within the blockchain ecosystem.

Device Differentiation: The first dimension shows how devices differ according to their performance, ability to interact with the external environment and communication capabilities. The main distinction between low-end, middle-end and high-end was explained in Chapter 4. Within the first dimension, the equipped systems can range from sensors that measure data from the environment or actuator, control and regulation systems that perform actions to maintain a desired state.

The used communication technologies represent a further distinguishing feature. The devices are equipped with at least one of the following communication technologies. Local Area Network (LAN) (e.g. Ethernet or bus systems) represents a wired communication technology. Personal Area Networks (WPAN) have a range of approx. 100 m and typical examples are Bluetooth, ZigBee or Z-Wave equipment. The IP-based network protocol 6LowPAN with its open IP standards and web sockets is also part of the WPAN. Wireless Local Area Networks (WLANs) with the most widespread Wi-Fi standard offer a range of up to 1 km. IoT devices can switch off Wi-Fi connections with the Target Wake Time function most of the time and only connect briefly and on schedule. Low-Power Wide Area Networks (LPWAN) is an emerging communication technology with extremely long battery life and a maximum communication range of over 20 km. The three most important competing standards are LoRa, Sigfox and NB-IoT. Wireless Neighborhood Area Networks (WNANs) lie between WLAN and long-range technologies such as mobile communications in terms of communication range. Typical representatives of this technology include mesh networks such as Wi-SUN or JupiterMesh. Mobile networks such as GSM, 3G, 4G and 5G are used for the long-range operation of IoT devices.

Network Integration: In a second dimension a distinction is made between the network and the gateway. The platform architecture of the IoT devices differs in terms of the use of a central node (e.g. with cloud architectures) or a decentralized IoT platform without a central node. Star, point-to-point and mesh are the three typical network topologies. In a star network, all devices are connected to a central hub. In point-to-point, a direct connection is established between the nodes. In the mesh network topology, all nodes can be connected to each other.

The next step is to take a closer look at blockchain. Blockchain governance is organized either via an independent blockchain network, a participating blockchain network as a connection to an existing blockchain network or as an integrated blockchain network. The distinction between light(weight) nodes and full nodes is particularly relevant for determining communication with the blockchain. The main difference is that, unlike a full node, a light(weight) node does not store the entire blockchain and can only send and process information.

IoT devices that are not clearly identifiable for the blockchain fall into the category of no node (e.g. via communication via an IoT cloud server). A cloud server, an enterprise server (with RPC function, for example), a light(weight) node or a full node can be used as a gateway to the blockchain. With the cloud server and company server, signing only takes place when the data is received by the central server. The full node must be located in the same local network as other IoT devices and is then responsible for signing, transmission and mapping (matching IoT device ID and private key). IoT devices with sensors and an integrated light(weight) node are also able to sign themselves and transfer the collected data to the blockchain, but light(weight) nodes cannot communicate with each other, i.e. with other light(weight) nodes.

Identification and Security: The third dimension comprises identification and security. The identification systems Self-Sovereign Identity (SSI), Bring Your Own Identity (BYOI), Public Key Infrastructure (PKI) and

Decentralized Public Key Infrastructure (DPKI) are used to give objects in cyber-physical systems a digital identity. With SSI, the user receives identity features and authorizations in the form of cryptographically secured digital proofs, which are called verifiable credentials, and can manage and verify these independently using a digital wallet without direct contact with the issuer. In this context, BYOI refers to the idea and goal of being able to use this personal identity in any environment, be it private or business, for online shopping or in an official context. PKI uses digital signatures as an identity. A private key, which is only in the possession of the user, enables content and documents to be signed. The public key allows anyone to verify the signature. The security of the infrastructure depends on the trustworthiness of the third party; DPKI addresses this weakness and uses a blockchain instead of key servers (third parties).

The guiding principle is the hierarchy-free web of trust, in which users confirm the credibility and accuracy of each other's data. Nodes participating in the blockchain are able to secure the origin and security of their collected data with their signature. This also works without publishing their own identity and with the help of various security mechanisms. For security and privacy in blockchain-based systems, the security mechanisms Anonymous Digital Signatures, Mixing, Homomorphic Encryption Algorithms, Secure Multiparty Computation Protocols or Non-interactive Zero-Knowledge Proof System can be integrated.

MD	Dimensions	Characteristics							MEX
Device Differentiation	Performance	Low-end Device		Middle-end Device		High-end Device			Y
	Equipped Systems	Sensor System		Actuator System		Control System	Regulation System	Visual Indication	N
	Communication Technologies	Wired				Wireless			N
		Local Area Network	Sigfox	Software Defined Networks		Personal Area Network	Wireless Area Network	Mobile / Neul	N
Network Integration	IT Architecture	Centralized				Decentralized			Y
	Network Topology	Star		Point-To-Point		Mesh			Y
	Blockchain Governance	Independent Blockchain-Network		Participating (Connection to existing Blockchain-Network)		Integrated (BaaS, Cloud-based)			Y
	Blockchain Types	Public Permissionless		Consortium		Private Permissioned			Y
	Blockchain Identifiability	No Node		Light(weight)-Node		Full-Node			Y
	Gateway	Cloud Server		Enterprise Server		Other Device	No Gateway		Y
Identification and Security	Identity Management	Self-Sovereign Identity		Bring Your Own Identity		Public Key Infrastructure	Decentralized Public Key Infrastructure		Y
	Security Mechanism	Anonymus digital signatures	Non-interactive zero-knowledge proofs	Homomorphic Encryption Algorithm		Secure multiparty calculation protocol	Attribute-based encryption algorithm	Mixing Procedures	N

Fig. 2: Blockchain Devices Taxonomy

6. Conclusion

In this paper, we have explored the landscape of blockchain devices, emphasizing their classification and the taxonomy that underpins their diverse applications. Through a detailed examination, we have identified and categorized these devices based on their type, integration level, and application domain, providing a comprehensive framework for understanding their roles and functionalities within the blockchain ecosystem.

Our analysis highlights the importance of distinguishing between various blockchain devices, including IoT devices, mobile devices, and specialized hardware, each serving distinct purposes and industries. The integration level—ranging from full nodes to light and hybrid nodes—plays a crucial role in defining their operational capabilities and resource requirements. Additionally, the application domains, such as supply chain management, environmental monitoring, compliance documentation, underscore the versatility and significance of these devices in real-world scenarios.

The proposed taxonomy not only aids in organizing existing blockchain devices but also paves the way for future research and development. By providing a structured approach to device classification, it enables researchers and practitioners to better understand the nuances of blockchain technology and its practical implementations. As blockchain continues to evolve, the insights derived from this taxonomy will be instrumental in advancing device design, enhancing functionality, and addressing emerging challenges in the field. In summary, this paper contributes to the body of knowledge on blockchain devices by offering a detailed classification and taxonomy, thus facilitating a deeper understanding and encouraging further exploration of this rapidly advancing technology.

References

[1] Hanseatic Blockchain Institute, Stand der Blockchain Adoption in der deutschen Wirtschaft, W3NOW.DE (2024).

[2] B. Teoh, Solving the blockchain oracle problem to enable supply chain mass adoption, AIP Conference Proceedings 2582 (2023).

[3] J. Maaßen, T. Gürpinar, M. Austerjost, J. Kamphues, Entwicklungsrahmen von Blockchain Devices, Scientific Report, Blockchain Navigator (2021).

[4] T. Gürpinar, M. Austerjost, J. Kamphues, M. Henke, Blockchain technology as the backbone of the internet of things – A taxonomy of blockchain devices, Conference on Production Systems and Logistics – CPSL (2022).

[5] A. Grünewald, T. Gürpinar, C. Culotta, Archetypes of blockchain-based business models in enterprise networks, Information Systems and e-Business Management (2024).

[6] A. Alphonse, M. Starvin, Blockchain and Internet of Things – An Overview (2020).

[7] T. Gürpinar, R. Ashraf, M. Henke, Integrating blockchain technology in supply chain management - a process model with evidence from current implementation projects, Hawaii International Conference on System Sciences (2024).

[8] E. Lichtenthaler, Methoden der Technologie-Früherkennung und Kriterien zu ihrer Auswahl, in: M. G. Möhrle, R. Isenmann (Eds.): Technologie-Roadmapping, 3rd ed, Berlin (2008), p. 59-84.

[9] D. Specht, S. Behrens, Integration der Technologieplanung in die strategische Geschäftsfeldplanung mit Hilfe von Roadmaps, in: M. G. Möhrle, R. Isenmann (Eds.): Technologie-Roadmapping, 3rd ed, Berlin (2008), p. 387-396.

[10] S. Lempert, IoT-Software-Plattformen: Methode zur Bewertung und Auswahl der am besten geeigneten Plattform, Springer Gabler Wiesbaden (2021).

[11] J. Gausemeier, C. Plass, Zukunftsorientierte Unternehmensgestaltung: Strategien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen, 2nd ed, Hanser (2014).

[12] R.C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, European Journal of Information Systems (2013).

[13] A. Vaghani, T. Gürpinar, N. Große, A Taxonomy Characterizing Blockchain-Empowered Services for the Metaverse, Blockchain and Cryptocurrency Conference (2022).

[14] M. Debe, K. Salah, R. Jayaraman, I. Yaqoob, J. Arshad, Trustworthy Blockchain Gateways for Resource-Constrained Clients and IoT Devices, IEEE Access (2021).

[15] C. Bormann, M. Ersue, A. Keranen, Terminology for Constrained-Node Networks, Internet Engineering Task Force (2014).

Integrating Blockchain Technology into WordPress for Self-Sovereign Identity: Development of a Verifiable Credential Validation Plugin

Anton Petzold, Jan Lippert
Hochschule Mittweida, Mittweida, Deutschland

The rapid digitalization of various sectors necessitates increasingly sophisticated methods for secure digital identity management. As traditional passwords are gradually deemed insecure, emerging technologies like Passkeys and Self-Sovereign Identity (SSI) are gaining prominence. This paper explores the theoretical foundations and potential implementation of a Verifiable Credential validation plugin for WordPress, which could serve as an alternative to existing authentication methods like Passkeys. The plugin aims to enable users to securely log in to websites by validating digital credentials within an SSI ecosystem. While the integration of SSI has been tested, the extension to include blockchain technology remains a theoretical proposal aimed at further enhancing security and decentralization. The discussion includes an analysis of potential blockchain platforms such as Ethereum, Hyperledger Fabric, and Polygon.

Die rasche Digitalisierung verschiedener Sektoren erfordert immer ausgefeiltere Methoden für ein sicheres digitales Identitätsmanagement. Da herkömmliche Passwörter allmählich als unsicher angesehen werden, gewinnen neue Technologien wie Passkeys und Self-Sovereign Identity (SSI) an Bedeutung. In diesem Beitrag werden die theoretischen Grundlagen und die potenzielle Implementierung eines Plugins zur Validierung von verifizierbaren Anmeldeinformationen für WordPress untersucht, das als Alternative zu bestehenden Authentifizierungsmethoden wie Passkeys dienen könnte. Das Plugin soll es Nutzern ermöglichen, sich sicher auf Websites anzumelden, indem digitale Anmeldedaten innerhalb eines SSI-Ökosystems validiert werden. Während die Integration von SSI bereits getestet wurde, bleibt die Erweiterung um die Blockchain-Technologie ein theoretischer Vorschlag, der darauf abzielt, die Sicherheit und Dezentralisierung weiter zu verbessern. Die Diskussion umfasst eine Analyse potenzieller Blockchain-Plattformen wie Ethereum, Hyperledger Fabric und Polygon.

1. Introduction

As digital identity management becomes increasingly important, the need for secure and user-friendly authentication methods is growing. Traditional password-based methods are increasingly being replaced by more secure alternatives, with passkeys and Self-Sovereign Identity (SSI) playing a prominent role. This paper builds on the concept of SSI and aims to develop a plugin to validate verifiable credentials for the WordPress content management system, which could serve as a secure and decentralized alternative to passkeys. While the integration of SSI into WordPress has already been successfully tested, this paper proposes the theoretical extension by integrating blockchain technology to further improve the security and decentralization of the system. Various blockchain platforms, including Ethereum, Hyperledger Fabric and Polygon, are discussed in terms of their potential use in this context (Petzold, 2023).

2. Background and Motivation

2.1 The Problem with Passwords

The ongoing issues surrounding password security highlight the growing inadequacy of traditional authentication methods. Passwords are susceptible to attacks, and even complex passwords fail to provide comprehensive protection against modern hacking techniques (Bonneau et al., 2012). Weaknesses in password-based systems have led to increasing interest in alternative forms of authentication that offer higher levels of security and user control.

2.2 The Rise of Self-Sovereign Identity

SSI represents a significant shift in how digital identities are managed. Unlike traditional identity systems that rely on centralized authorities, SSI gives users control over their own digital identities. This is achieved through the use of Verifiable Credentials, which allow users to prove their identity without relying on third parties. By enabling users to manage their identities independently, SSI reduces the risk of data breaches and increases user privacy (Preukschat & Reed, 2021).

2.3 Motivating the Use of blockchain

Blockchain technology has emerged as a potential solution to several challenges related to digital identity management. Its decentralized nature combined with its ability to provide immutable and transparent records makes it an attractive option for improving SSI systems. However, the integration of blockchain into the proposed plugin remains theoretical and is proposed as a future enhancement to strengthen the security and trustworthiness of the system (Nakamoto, 2008; Treiblmaier & Önder, 2019).

3. Technological Foundations

3.1 Passwordless login procedures

Passwordless login procedures have become considerably more important in recent years as they offer improved user-friendliness and greater security. These methods are usually based on authentication by possession (such as smartphones or hardware tokens) or biometrics (e.g. fingerprint, facial recognition). Such technologies make it possible to grant users access without them having to remember or enter complex passwords. An example of a widely used passwordless technology is the Passkey method introduced by companies such as Google and Apple (Ping Identity, n.d.).

3.2 Passkey Technology

The passkey method works with an asymmetric cryptographic key pair consisting of a private and a public key. The private key is stored securely on the user's end device and never leaves it. The public key is transmitted to the service provider. When logging in, the end device signs a request initiated by the service with the private key. The service verifies the signature with the public key and grants access if the verification is successful. As the private key never leaves the device, the process offers a high level of security. (FIDO Alliance, 2022).

3.3 Self-Sovereign Identity (SSI)

The concept of Self-Sovereign Identity (SSI) offers a comprehensive solution for managing digital identities that goes far beyond mere authentication. In contrast to traditional identity providers that store data centrally, SSI enables users to manage their identities and personal data decentrally and independently. Verifiable credentials, which are created by the issuer and stored in a user's SSI wallet, can be securely passed on to third parties, the authenticator, if required. The three actors - issuer, authenticator and user - together form the so-called Trust Triangle. This means that the user retains full control over their identity and the transfer of their data, which guarantees greater security and autonomy. In contrast to passkey procedures used by large corporations, no company infrastructure is required for communication between the players. Instead, communication can be realized via a blockchain or peer-to-peer without any additional infrastructure. This would make such a solution much more independent and decentralized. This would also reduce the risk of failure, as only the actors involved would be affected in the event of a major system failure and the entire system would not be paralyzed across the board. (Preukschat & Reed, 2021).

3.4 Blockchain Technology

Blockchain is a decentralized and immutable database technology characterized by its transparency, security, and decentralization. In the context of SSI, blockchain offers a robust infrastructure for managing and verifying Verifiable Credentials. By integrating blockchain, the validation processes of the plugin could be additionally secured and made transparent. However, this integration remains a theoretical extension aimed at exploring the potential benefits of blockchain in enhancing SSI systems (Nakamoto, 2008; Treiblmaier & Önder, 2019). Recent research emphasizes that blockchain serves as the backbone for SSI by ensuring the integrity and interoperability of identity credentials, which is crucial for the adoption and success of SSI solutions (Trust Models in Blockchain-Based SSI, 2024).

4. Integrating Blockchain Research

Verifiable Credentials are closely linked with blockchain technology, as they are based on the principles of decentralization, security, and transparency enabled by blockchain. Blockchain can be used to ensure the authenticity of Verifiable Credentials by cryptographically signing and storing them in an immutable and transparent manner (Erceg et al., 2020). The SSI ecosystem, which uses Verifiable Credentials, could benefit from blockchain technology by creating a decentralized trust network that does not rely on central authorities (Nam et al., 2019). A recent study highlights that blockchain is fundamental for decentralized digital identity management, enabling users to maintain full control over their data while ensuring security and verifiability (Blockchain as the Backbone for SSI, 2023).

5. Discussion of Blockchain Platforms: Ethereum, Hyperledger Fabric, and Polygon

When considering the integration of blockchain into the SSI-based WordPress plugin, several blockchain platforms present themselves as viable options, each with unique strengths and challenges.

5.1 Ethereum

Ethereum is a well-established, public blockchain platform known for its support of smart contracts—self-executing contracts with the terms of the agreement directly written into code. Ethereum's smart contract functionality is particularly valuable for SSI systems, allowing the automation of identity verification processes without the need for intermediaries. The platform's maturity and extensive developer ecosystem make it a strong candidate for integrating blockchain into the SSI plugin. Additionally, Ethereum's adoption of standards such as ERC-20 and ERC-721 ensures interoperability, which is crucial for systems that require interaction across multiple applications and networks. However, Ethereum's scalability issues and high transaction costs on the mainnet could pose challenges, especially in high-volume scenarios (Buterin, 2014).

5.2 Hyperledger Fabric

Hyperledger Fabric is a permissioned blockchain platform, making it distinct from Ethereum's public, permissionless network. This characteristic of Hyperledger Fabric allows for a more controlled environment, where participants are known and trusted. This could be

particularly advantageous for enterprise-level implementations of the SSI plugin, where privacy and compliance with regulatory requirements are paramount. Hyperledger Fabric's modular architecture allows developers to customize components such as consensus mechanisms and membership services, which could be tailored to meet the specific needs of an SSI system. However, the permissioned nature of Hyperledger Fabric might limit the degree of decentralization and could introduce challenges related to interoperability with other blockchain networks (Androulaki et al., 2018).

5.3 Polygon

Polygon (formerly Matic Network) is a Layer 2 scaling solution designed to improve Ethereum's scalability and reduce transaction costs. It operates on top of the Ethereum blockchain, providing faster and cheaper transactions while maintaining compatibility with Ethereum's ecosystem. For the SSI plugin, Polygon could offer a balance between the security and functionality of Ethereum and the need for scalable, cost-effective operations. By leveraging Polygon, the plugin could benefit from the robust Ethereum network while avoiding the high costs and slower transaction times associated with Ethereum's mainnet. This makes Polygon a compelling option for scenarios where the plugin needs to handle large volumes of transactions or where cost sensitivity is a concern (Jani, 2017).

6. Concept of the Validation Plugin

6.1 Plugin Overview

The plugin developed for WordPress is intended to provide a secure and user-friendly method of authentication by validating Verifiable Credentials within an SSI ecosystem. The plugin integrates with the Gutenberg editor of WordPress, allowing website owners to create custom validation processes for accessing protected content. The SSI integration has been tested successfully, demonstrating the plugin's ability to enhance security and user control. The proposed extension to include blockchain technology remains theoretical, aimed at exploring how platforms like Ethereum, Hyperledger Fabric, or Polygon could further improve these aspects (Petzold, 2023).

6.2 Registration and Integration into WordPress

The plugin is designed as an extensible add-on that can be easily integrated into existing WordPress websites. It utilizes the WordPress API to seamlessly interact with other plugins and themes. The current implementation focuses on SSI without blockchain, but the potential integration of blockchain networks for managing Verifiable Credentials is discussed as a future enhancement. Each of the discussed platforms—Ethereum, Hyperledger Fabric, and Polygon—offers unique benefits that could be leveraged depending on the specific requirements of the deployment (Petzold, 2023; Nakamoto, 2008).

6.3 Validation Process

The validation process occurs in real-time by matching the Verifiable Credentials provided by the user with the website's requirements. The current system successfully uses SSI to verify credentials, and only upon successful validation does the user gain access to protected content. The theoretical integration of blockchain would involve using platforms like Ethereum for smart contract execution, Hyperledger Fabric for a permissioned, private environment, or Polygon for scalable, low-cost operations. The validation process occurs in real-time by matching the Verifiable Credentials provided by the user with the website's requirements. The current system successfully uses SSI to verify credentials, and only upon successful validation does the user gain access to protected content. The theoretical integration of blockchain would involve using platforms like Ethereum for smart contract execution, Hyperledger Fabric for a permissioned, private environment, or Polygon for scalable, low-cost operations. Each platform's suitability depends on the specific needs of the implementation, such as the level of decentralization required, transaction costs, and scalability considerations (Treiblmaier & Önder, 2019; Buterin, 2014; Jani, 2017).

7. Application Possibilities and Comparison with Passkeys

7.1 Application Possibilities

Decentralized management of digital identities

The management of digital identities through SSI opens up numerous possibilities that go far beyond mere authentication. By using SSI, companies and organizations can decentralize the management of user accounts and thus significantly improve the security and privacy of their users. This could be used in areas such as e-government, e-health or education, for example, where users can prove their identity securely and easily without having to pass on their sensitive data to central authorities. But it could also be used in the field of e-commerce to prove ownership of a user account and simplify digital payments.

Data protection and security

One of the biggest advantages of SSI is data protection and data security. As the data is stored decentral on the user's devices and not in central databases, the risk of data leaks and unauthorized access is significantly reduced. Only the user decides who can access which data and can revoke this at any time. Passkey technologies also offer a high level of security by eliminating the need for passwords and thus removing one of the biggest weaknesses in IT security.

Data economy and transparency

SSI can lead to a new form of data economy in which users themselves decide what data they disclose and how it is used. This could be particularly beneficial in the area

of personalized advertising or participation in data ex-change platforms, where users could be remunerated for the use of their data. The transparency this creates enables users to keep track of their data and ensure that it is only used for their benefit.

7.2 Comparison with Passkeys

Compared to Passkeys, the SSI-based plugin offers sev-eral advantages, including greater user control over data and better integration into decentralized systems. The potential integration of blockchain technology could am-plify these advantages by adding an additional layer of security and transparency. However, the use of block-chain would also introduce challenges, particularly in terms of user-friendliness and the complexity of imple-mentation. Ethereum's public nature might raise con-cerns about privacy and transaction costs, while Hy-perledger Fabric's permissioned nature could limit ac-cessibility. Polygon, while cost-effective, might require additional layers of integration to fully utilize its capabil-ities in conjunction with Ethereum's ecosystem (FIDO Al-liance, 2022).

8. Implementation and Testing

8.1 SSI Integration and Testing

The prototype of the plugin was successfully imple-mented and tested in an environment to ensure func-tionality and security. The testing focused on the integra-tion of SSI and demonstrated that the plugin could effec-tively validate Verifiable Credentials and provide secure authentication on WordPress websites.

8.2 Theoretical Blockchain Integration

The theoretical extension of the plugin to include blockchain was analyzed based on its potential benefits and challenges. While the concept of integrating blockchain into the plugin is promising, particularly for enhancing security and decentralization, it has not yet been tested. Theoretical models suggest that blockchain could provide an immutable record of all credential validations, ensuring transparency and trust in the authentication process. However, practical implementation would require addressing potential issues such as scalability, user-friendliness, and integration with existing systems. This remains an area for future research and development, with the aim of determining the feasibility of such an integration and testing its effectiveness in real-world scenarios (Blockchain as the Backbone for SSI, 2023).

9. Conclusion and Outlook

The increasing prevalence of digital identities and the need for strong data protection make new technologies such as SSI and Passkeys indispensable tools in the mod-ern IT landscape. SSI offers a revolutionary concept that puts the power over personal data back in the hands of the user while increasing security. Passkeys provide a straightforward alternative that removes the complexity of passwords and increases ease of use. The future of these technologies will depend on how well they can be integrated into existing systems and how successfully the associated challenges are overcome. Widespread ac-ceptance will ultimately depend on how easily and se-curely these technologies can be used in practice and how they are made accessible.

This work has shown that verifiable credentials in com-bination with SSI represent a robust alternative to con-ventional authentication methods. The WordPress plugin developed as part of this work provides a secure and user-friendly way to integrate these technologies into existing websites. The successful testing of SSI inte-gration underlines the practical benefits of this ap-proach, particularly in improving security and user con-trol over digital identities.

The integration of blockchain technology, although still theoretical at present, represents a significant potential improvement to the system. By leveraging the decentral-ized and immutable nature of blockchain, the plugin could provide even more security and transparency in the management of digital identities. Ethereum, Hy-perledger Fabric and Polygon each represent viable op-tions for this integration, depending on the specific re-quirements of the system, such as the level of decentral-ization required, transaction costs and scalability. How-ever, this approach requires further research to address the practical challenges associated with blockchain inte-gration, including scalability, user adoption and system complexity.

Acknowledgements

In the preparation of this work, the assistance of an arti-ficial intelligence (AI) model, specifically OpenAI's ChatGPT, was utilized for generating text and refining content. The final responsibility for the content rests with the author(s).

References

[1] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy (pp. 553-567). IEEE.

[2] Erceg, V., et al. (2020). The impact of blockchain on tourism: Automation, security, and trust. *Information Technology & Tourism.*

[3] FIDO Alliance. (2022). FIDO2: Web Authentication (WebAuthn) and CTAP. Retrieved from https://fidoalliance.org/

[4] Garman, C. (2016). SSL and TLS essentials: securing the web. John Wiley & Sons.

[5] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[6] Nam, K., Dutt, S. C., Chathoth, P., & Khan, S. M. (2019). Blockchain technology for smart cities and smart tourism: Latest trends and challenges. Journal of Asia-Pacific Tourism Research.

[7] Petzold, P. W. A. (2023). Development of a Verifiable Credential Validation Plugin for WordPress for Secure Login Compared to Passkey Technologies. Bachelor's thesis, Mittweida University of Applied Sciences.

[8] Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity: Decentralized digital identity and verifiable credentials. Manning Publications.

[9] Treiblmaier, H., & Önder, I. (2019). The impact of blockchain on the tourism industry: A framework and research agenda. Annals of Tourism Research.

[10] Valeri, M., & Baggio, R. (2021). Blockchain and the tourism value chain: Disintermediation, data privacy, and consumer empowerment. Information Technology & Tourism.

[11] Trust Models in Blockchain-Based SSI. (2024). Journal of Blockchain Technology.

[12] Blockchain as the Backbone for SSI. (2023). *International Journal of Digital Identity Management*.

[13] Ping Identity. (n.d.). Passwordless authentication (Whitepaper). Retrieved from https://inhalte.pingidentity.com/white-papers/3480-passwordless-authentication

Offlinefähige Schließanlagen auf Blockchain-Basis

Robert Manthey, Richard Vogel, Matthias Vodel
Fakultät für Computer- & Biowissenschaften, Hochschule Mittweida, Deutschland

Abstract
Permission management for access of rooms, laboratories etc. is a cost and time-consuming task with common systems in large facilities. Especially, frequent changes and staff turnover need proper and efficient workflows and extensive logistics. The interconnection of common electronic locking systems with blockchain based permission data management and smartphones makes it possible to reduce the needed resources as well as entry point for tampering permissions.

Kurzfassung
Das Berechtigungsmanagement für den Zugang zu Räumen, Laboren etc. ist mit üblichen Systemen eine kosten- und zeitintensive Aufgabe in großen Einrichtungen. Insbesondere häufige Wechsel und Fluktuationen des Personals erfordern gut strukturierte und effiziente Arbeitsabläufe und eine umfangreiche Logistik. Die Verknüpfung gängiger elektronischer Schließsysteme mit Blockchain-basiertem Berechtigungsdatenmanagement und Smartphones ermöglicht es, die benötigten Ressourcen sowie die Einstiegspunkte für Manipulationen zu reduzieren.

1. Einleitung

Große Unternehmen und Institutionen verteilen sich typischerweise über eine Vielzahl an Gelände mit verschiedenen Bereichen mit jeweils spezifischen Zugangsberechtigungen für Labore, Gebäude oder Zweigstellen. In einem Gebäude kann beispielsweise der Zugang zu Raum 213 auf die Mitarbeiter einer Abteilung beschränkt werden, während das Reinigungspersonal Zugang zu allen Räumen im dritten Stock des Hauptgebäudes freitags von 17:00 bis 19:00 Uhr erhält, wie in Abbildung 1 dargestellt. Darüber hinaus können das Sicherheitspersonal sowie Personen mit besonderen Qualifikationen, alle Räume in diesem Gebäude betreten. Reguläres Personal sollten hingegen nur Zugang zu den Räumlichkeiten haben, die zur Erfüllung ihrer Aufgaben benötigen. Diese Zugangsberechtigungen werden oft mittels Schließsystemen realisiert, welche von einer Vielzahl von Herstellern mit einer Vielzahl von Systemen und Schlüsselausstattungen angeboten werden. Sie decken einen breiten Bereich an Anwendungsbereich ab und bieten bewährte Lösungen an.

Allerdings führen häufige Änderungen beim Personal oder den Berechtigungen zu einem beträchtlichen Verwaltungsaufwand und erhebliche Kosten[1] [2]. Ebenso wie bei Verlusten oder Diebstahl[3] müssen dann größere Mengen an Schlüsseln und Schlössern der betroffenen Organisationsbereiche, Abbildung 2, erneuert bzw. reprogrammiert werden. In dieser Hinsicht bieten elektronische Schließsysteme zwar erhebliche Zeit- und Kosteneinsparungen. Sie erfordern jedoch in der Regel eine Datenverbindung zwischen der Verwaltungszentrale und den betroffenen Schlössern, wodurch erhebliche Investitionen in die eingesetzte Infrastruktur notwendig sind.

Die im Rahmen dieser Arbeit erstellte Lösung kombiniert bestehende Schlösser und der damit einhergehenden Sicherheit, Leistungsfähigkeit, Flexibilität und einfachen Aktualisierbarkeit der Berechtigungsdaten mit den dezentralen, manipulationsresistenten Eigenschaften der Blockchaintechnologie, sowie den weitverbreiteten, mit beträchtlichen Speicher- und Rechenressourcen ausgestatteten Smartphones der Schließanlagennutzer.

Abbildung 1: Beispielhafte Verteilung von Schließberechtigungen (rot, grün, blau, hellblau, violett) an vier Standorten mit Gebäude, Türen und Fenster. Bestimmte Berechtigungen außerdem unterliegen zeitlichen Einschränkungen. [1]

[1] https://www.forbes.com/home-improvement/home-security/cost-to-hire-a-locksmith/
[2] https://vizpin.com/blog/access-control-pricing/
[3] https://www.verbraucherzentrale.de/wissen/geld-versicherungen/weitere-versicherungen/generalschluessel-verloren-drohende-kosten-bis-zum-preis-eines-kleinwagens-10679

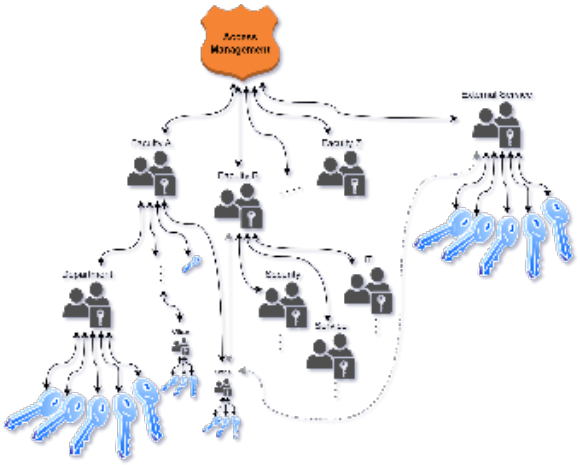

Abbildung 2: Hierarchie der Organisationsbereiche mit der Gruppierung der Zugangsberechtigungen und mehrfachen Zugehörigkeiten. Unterschiedliche Schlüssel repräsentieren die jeweiligen Berechtigungen. [7]

2. Grundlagen

Für die Steuerung des Zugangs zu Gebäuden und Räumen werden häufig klassische mechanische Schließanlagen auf Basis des berechtigten Besitzes von administrativ eingestellten Schlüsseln verwendet. Diese sind zwar vergleichsweise kostengünstig[4], aber unflexibel. Die physischen Schlüssel können unbemerkt kopiert und Kreis der Zugangsberechtigten unerlaubt erweitert werden, was nur durch den aufwändigen Austausch aller möglicherweise betroffenen Schlösser vermieden werden kann.

Elektronische Schließanlagen wie blueSmart von WINKHAUS[5] oder blueSmart von WINKHAUS[6] stellen zwar mehr Flexibilität zur Verfügung, erfordern aber entweder ein individuelles Reprogrammieren bei Änderungen und somit vertrauenswürdiges Personal und Zeit, oder permanent verfügbare Infrastruktur in Form von Kommunikation mit der Verwaltungszentrale, was beträchtliche Kosten verursacht. Lokkit[7] stellt behebt etliche dieser Nachteile zwar, nutzen aber das Smartphone des Nutzers für Verifikationsaufgaben, sodass Dritten vertraut werden muss.

Die von [4] vorgestellte Technologie der Blockchain behebt diese Nachteile und erlaubt eine gesicherte Übertragung der Berechtigungsdaten über ungesicherte Zwischenstellen und in sehr hohem Maße abgesichert gegen unentdeckte Manipulation. Daten werden hierbei in Transaktionen strukturiert und in Blöcken zusammengefasst an eine Menge von Knoten gesandt, welche daraus

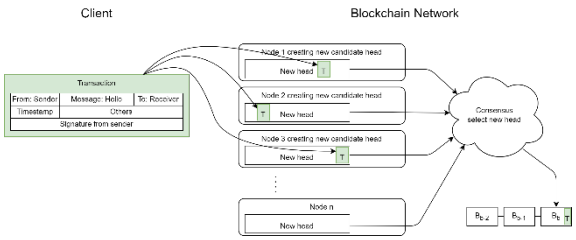

Abbildung 3: Nutz- und Metadaten als Transaktion zusammengefasst werden als Bestandteil in neue Blockkopfkandidaten kombiniert. Durch den Konsensus wird der neue Kopf gewählt und die Blockchain verlängert. [8]

einen neuen Kopf der Blockchain erzeugen. Durch die Verkettung der Blöcke wird eine Absicherung gegen Manipulation erzeugt, wie in Abbildung 3 dargestellt. Erweiterungen der Funktionalität der Blockchain-Technologie ermöglichen außerdem bedingte Transaktionsausführungen, Smart Contracts oder auch verteilte Identitätsprüfung. [2,3,5,6]

3. Realisierung

Für die Verwaltung der Schließberechtigungen, als auch für die Anforderung einer Schließaktion wurde eine auf dem Flutter-Framework[8] basierende Smartphone-App erstellt. Die Nutzer können gruppiert und so mit den notwendigen Eigenschaften des gewährten Zutritts ausgestattet werden, wie in Abbildung 4 dargestellt.

Diese Daten werden an den von der Verwaltung festgelegten Speicherplatz für die Off-Chain-Daten übermittelt, entsprechend des Workflows in Abbildung 5. Zusätzlich erfolgt die Erstellung der Sicherheitsinformationen mittels Hashes und deren Übermittlung als Transaktion an die Ethereum-Blockchain[9].

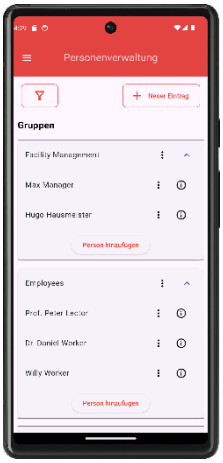

Abbildung 4: Beispiel der Gruppierung von Nutzern in Gruppen denen gleiche Schließberechtigungen zugewiesen wurden.

[4] https://kiwi.ki/schliessanlage/kosten
[5] https://www.winkhaus.com/de-de/zutrittsorganisation/elektronische-zutrittsorganisation/elektronische-schliesssysteme/bluesmart
[6] https://www.winkhaus.com/de-de/zutrittsorganisation/elektronische-zutrittsorganisation/elektronische-schliesssysteme/bluesmart
[7] https://news.hslu.ch/siemens-zeichnet-projekt-von-informatik-absolventen-aus/
[8] https://www.flutter.dev/
[9] https://www.ethereum.org/en/

Der Nutzer lädt regelmäßig die aktuellen Daten vom Off-Chain-Speicherplatz und den aktuellen Stand der Blockchain auf sein Smartphone, wenn eine Verbindung zum Netzwerk verfügbar ist. Sobald das Smartphone in Reichweite eines Schlosses ist, erfolgt eine Übermittlung der Daten des Smartphones mittels Bluetooth LE[10]. Das Schloss, welches über keine weiter Verbindungen verfügt, verifiziert die Korrektheit der empfangenen Daten und aktualisiert seine internen Daten der Zugangsberechtigten und den Stand der Blockchain. Die Eigenschaften der Blockchain und die Hashes der Daten der Zugangsberechtigten verhindern eine unerkannte Manipulation.

Mittels der App fordert der Nutzer eine Schließaktion beim Schloss an und liefert dabei die notwendigen Beweise seiner Identität, welche vom Schloss geprüft werden. Verbindungen zum Netzwerk, der Zugriffsverwaltung oder Datenspeichern ist nicht notwendig. Liegen ebenfalls die entsprechenden Berechtigungen vor, so führt das Schloss die angefragte Aktion aus.

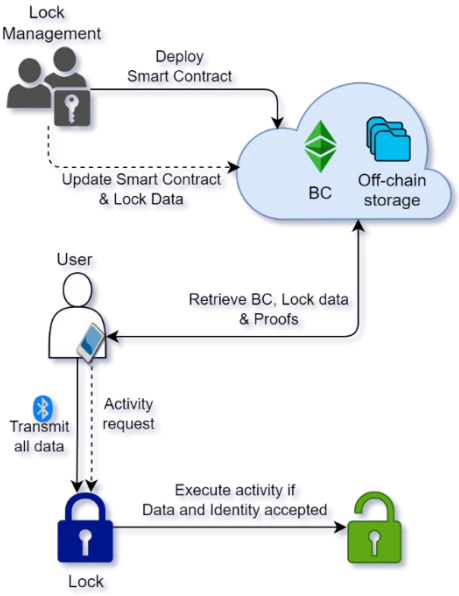

Abbildung 5: Schematischer Ablauf der Verteilung der Schließberechtigungen von der Erstellung durch das Management, über die Speicherung der Daten sowie ihrer Verifikationsinformationen in der gewählten Blockchain bis hin zum Download der notwendigen Informationen durch den Nutzer mit dem späteren Transfer zum Schloss. Hier erfolgt die Prüfung der Daten und gegebenenfalls die Aktionsausführung. [9]

4. Zusammenfassung und Ausblick

Bisherige Schließanlagen waren schwer zu aktualisieren oder benötigten zusätzliche Infrastruktur, was durch die hier vorgestellte blockchainbasierte Weiterentwicklung effizient gelöst wird. Durch die Verwendung des Smartphones des Nutzers, u.a. als Transportmedium, sind keine weiteren Komponenten erforderlich und das Schloss damit offline. Gleichzeitig ist die Aktualität der Schließberechtigungen gewährleistet. Aufgrund der Anforderungen an die Hardware sind zukünftig Optimierungen und Beschleunigungen der Datenübertragungen und des Energieverbrauchs vorgesehen.

Danksagung

Diese Arbeit wurde teilweise im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts *Chainlock - Blockchain-gestützte, smarte Schließanlagen* (Projektnr. 8233216) durchgeführt.

Literaturverzeichnis

[1] R. Manthey, R. Vogel, and M. Vodel, “Chainlock – Blockchain-gestützte, smarte Schließanlagen,” in Konferenzband zum Scientific Track der Blockchain Autumn School 2023, vol. 2. Hochschule Mittweida, p. 4.
[2] Christian Cachin and Marko Vukolić. 2017. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873
[3] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access 7 (2019), 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
[4] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (03 2009), 9 pages. https://bitcoin.org/bitcoin.pdf
[5] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2021. Decentralized Identifiers (DIDs) v1.0. W3C. https://www.w3.org/TR/2021/CRD-did-core-20210529/
[6] N. Szabo. 1994. Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
[7] R. Manthey, R. Vogel, M. Baumgart, C. Roschke, M. Ritter, M. Vodel. 2023. Decentralized Resilient Smart Lock System with Offline Capabilities – ChainLock. In Proceedings of the 16th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA) 5-7 July 2023, Corfu Island, Greece
[8] R. Manthey, R. Vogel, F. Schmidsberger, M. Baumgart, C. Roschke, M. Ritter, and M. Vodel, “Blockchain based social commitment-secure & reliable web services,” in International Workshop on Metrology for Living Environment (MetroLivEn). New York, NY, USA: IEEE, 07 2022, pp. 101–104.
[9] R. Vogel, R. Manthey, M. Baumgart, C. Roschke, M. Ritter, and M. Vodel, “Tamperproof data transmission to offline IoT devices in a zero-trust environment,” in 2024 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2024, pp. 817–822. [Online]. Available: http://www.conf-icnc.org/2024/papers/p817-vogel.pdf

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3478807/

Blockchain Basierter Biomassenachweis (BBBio) - Eine innovative Lösung?

Volker Wannack
Hochschule Mittweida, Mittweida, Deutschland

Der „Blockchain-basierte Biomassenachweis“ (BBBio) zielt darauf ab, die Biomassezertifizierung grundlegend zu modernisieren, indem er Blockchain-Technologie, Smart Contracts, IoT und Zero-Knowledge-Proofs (ZKP) integriert. Diese innovative Kombination führt zu einer erheblichen Effizienzsteigerung in der Biomasse-Ökonomie, indem sie bürokratische Prozesse automatisiert und Transparenz sowie Rückverfolgbarkeit entlang der gesamten Wertschöpfungskette der Biogasproduktion verbessert. Der entwickelte Minimum Viable Product (MVP) optimiert nicht nur bestehende Abläufe, sondern fördert auch die regionale Wirtschaft durch die Schaffung neuer Arbeitsplätze und intensiviert den Wissenstransfer zwischen Forschung und Industrie, was den Bereich nachhaltiger Biomassezertifizierung nachhaltig stärkt.

1. Einleitung

Das Projektvorhaben, dass im Rahmen des Förderprogramms „WIR! – Wandel durch Innovation in der Region“ „WIR!“ des Bundesministerium für Bildung und Forschung (BMBF), hat das Ziel, die herkömmliche komplexe Biomassezertifizierung durch eine innovative Blockchain-basierte Lösung namens "Blockchain-basierten-Biomassenachweis" (BBBio) zu revolutionieren. Die technischen Schlüsselkomponenten, die dieses Vorhaben unterstützen, sind Smart Contracts, IoT-Technologien und Zero-Knowledge-Proofs (ZKP).

Der Kern dieses Projekts liegt in der signifikanten Steigerung der Effizienz für Anlagenbetreiber und Landwirte in der Biomasse-Ökonomie. In diesem Zusammenhang werden zeitintensive bürokratische Prozesse und manuelle Dokumentationsverfahren durch automatisierte Abläufe und smarte Sensorgeräte ersetzt und optimiert. Gleichzeitig wird eine bislang unerreichte Verbesserung der Transparenz, Digitalisierung und Effizienz in Bezug auf die Dokumentation und Rückverfolgbarkeit der Biogasproduktion und -verwendung erzielt. Dies ermöglicht eine vereinfachte und kostengünstigere Ausstellung von Nachhaltigkeitszertifikaten wie Proof of Sustainability (PoS) und gewährleistet gleichzeitig ein höheres Maß an Transparenz und Rückverfolgbarkeit.

Im Detail erstreckt sich das übergeordnete Ziel dieses Projekts auf die Entwicklung eines funktionsfähigen und praxistauglichen BBBio-MVP, das durch seine Implementierung eine Reihe bisher unerreichter Alleinstellungsmerkmale, Vorteile und Mehrwerte realisiert: Erstens vereint das BBBio-MVP Lieferketten, um die Energieeffizienz der gesamten Biogasproduktion und -nutzung zu steigern. Es vereinfacht die Kommunikations- und Kooperationsprozesse zwischen allen beteiligten Unternehmen, wodurch die gesamte Wertschöpfungskette effizienter gestaltet wird. Zudem unterstützt es den grünen Transformationsprozess durch transparente und nachvollziehbare Daten und reduziert erheblich die Möglichkeiten für Betrug, da Falschangaben schnell erkannt werden und bei Unregelmäßigkeiten keine Zertifizierung erfolgt. Dieser Ansatz schafft einen

nahtlosen, digitalen Workflow, der von der Abfallentsorgung über die Gaserzeugung bis hin zur Energieeinspeisung und Outputstoffverwertung reicht. Jeder Schritt dieses Prozesses wird auf der Blockchain erfasst, was eine lückenlose Rückverfolgbarkeit ermöglicht. Die derzeit aufwendigen und zeitintensiven Zertifizierungsprozesse werden durch die Blockchain-Technologie vereinfacht, was zu einer erheblichen Effizienzsteigerung bei allen Biogasanlagen in Deutschland und Europa führt. Zweitens kann die Implementierung des BBBio-MVP zur Gründung einer Blockchain-Betreiber- und Consultinggesellschaft führen. Die kann sich mit Expertise in der dezentralen Energieversorgung rühmen und schafft langfristige attraktive und nachhaltigkeitsorientierte Arbeitsplätze. Drittens ermöglicht das BBBio-MVP die Entstehung neuer tragfähiger Geschäftsmodelle auf Grundlage konkreter Ergebnisse. Diese Geschäftsmodelle bilden die Grundlage für weitere Unternehmensansiedlungen und Neugründungen, was zur zusätzlichen langfristigen Schaffung von Arbeitsplätzen beiträgt. Viertens trägt das BBBio-MVP signifikant zur Steigerung der Wertschöpfung bei, indem es einen technologischen und wirtschaftlichen Vorsprung schafft. Dies führt zu einer verbesserten nationalen und internationalen Sichtbarkeit und etabliert die BBBio als Vorreiter und Leuchtturm mit überregionaler Strahlkraft. Fünftens motiviert die Entwicklung des BBBio-MVP zu verstärkter Forschung und Entwicklung und trägt zur Verbesserung und Bündelung des Wissenstransfers zwischen Hochschulen und Unternehmen bei. Dies steigert die wissenschaftliche Leistungsfähigkeit und entspricht dem Verständnis von strategischem Innovationsmanagement und Innovationskultur des Freistaates Sachsen. Es bündelt zwei zukunftsweisende Technologien im innovativen Rahmen der Sektorkopplung auf übergeordneter Ebene.

2. Stand der Wissenschaft und Technik

Gemäß den Richtlinien, die in Abbildung 1 dargestellt sind, sind die Mitgliedsstaaten der Europäischen Union durch den regulatorischen Rahmen der Renewable Energy Directive II (RED II) [1] verpflichtet, nachhaltige Biomasseinputstoffe gemäß den spezifischen Kriterien der EU-Richtlinie 2009/28/EG [2] zu zertifizieren und in einem nationalen Register zu verwalten. Diese Verpflichtung stellt eine fundamentale Komponente des europäischen Energienetzes dar, das durch einen komplexen internationalen Austausch von Zertifikaten und Energie gekennzeichnet ist. Die Implementierung dieses Systems beginnt auf regionaler Ebene und erfordert eine enge Abstimmung und Koordination zwischen den verschiedenen nationalen und europäischen Instanzen.

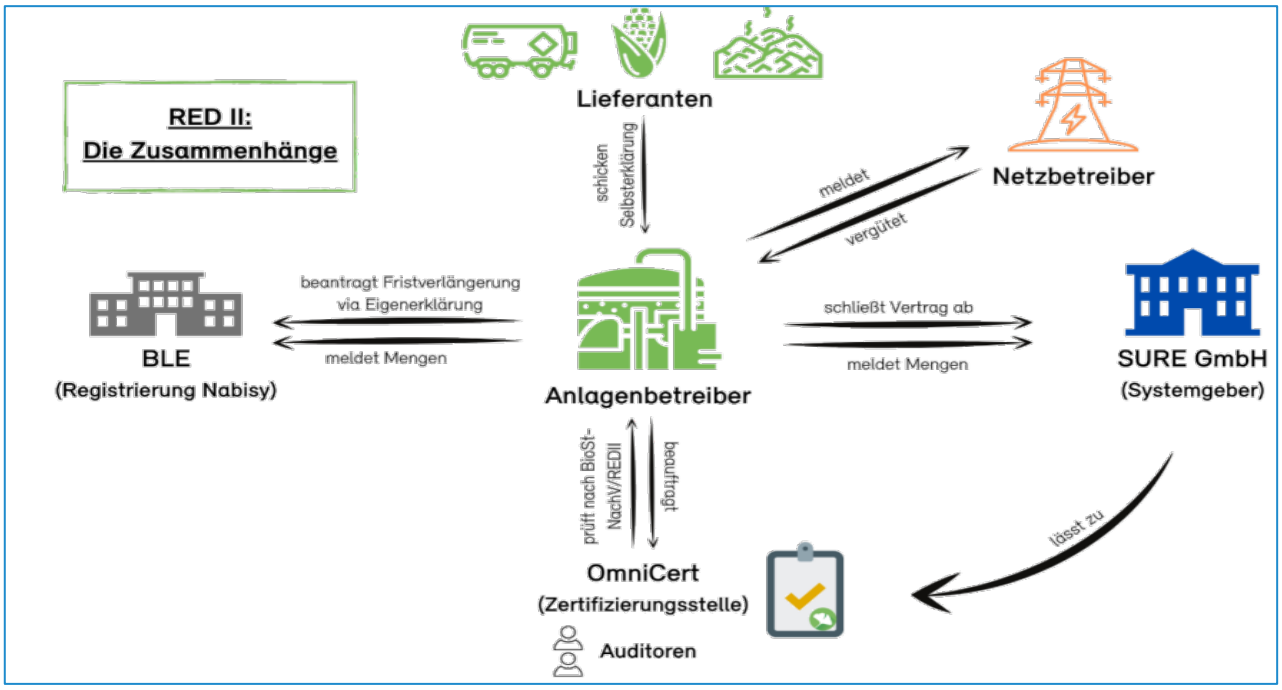

Abbildung 1: derzeitiger Biomassenachhaltigkeitsnachweisprozess (Eigene Darstellung)

Es ist jedoch zu beachten, dass der genaue Gestaltungsrahmen für die jeweilige Zertifizierungssystematik nicht explizit in allen Einzelheiten vorgeschrieben ist. Diese Regelung führt zu erheblichen Variationen in der praktischen Umsetzung und den spezifischen Anforderungen der Zertifizierungssysteme zwischen den europäischen Mitgliedsstaaten. Während die RED II die allgemeinen Rahmenbedingungen festlegt, bleiben die Details und die spezifische Ausgestaltung der Zertifizierungssysteme den einzelnen Mitgliedsstaaten überlassen. Diese Flexibilität kann zu Unterschieden in der Effizienz und Transparenz der Zertifizierungsprozesse führen, was in der Praxis Herausforderungen bei der einheitlichen Überwachung und dem internationalen Austausch von Biomassezertifikaten mit sich bringt.

In Deutschland sind die Biogasanlagenbetreiber gesetzlich verpflichtet, Biomassenachhaltigkeitsnachweise im Biogasregister „Nachhaltige-Biomasse-Systeme“ (Nabisy) [3] für jede Inputstoffmenge pro Blockheizkraftwerk (BHKW) regelmäßig vorzulegen. Die Nachweise müssen quartalsweise bei der Bundesanstalt für Landwirtschaft und Ernährung (BLE) eingereicht und zudem jährlich an die SURE GmbH übermittelt werden. Diese Nachweise werden von akkreditierten Zertifizierern überprüft und auditiert, um die Konformität mit den festgelegten Nachhaltigkeitskriterien sicherzustellen. In diesem Zusammenhang bestehen enge Verbindungen und Arbeitsbeziehungen zwischen dem Betreiber des Nabisy-Registers und der Firma Ökotec, die für die praktische Umsetzung und Verwaltung der Nachweise von zentraler Bedeutung sind.

Der bestehende Zertifizierungsprozess umfasst eine Vielzahl von Stakeholdern innerhalb der komplexen Wertschöpfungskette der Biomasseproduktion. Diese Stakeholder sind auf gegenseitiges Vertrauen angewiesen, welches jedoch oft nicht ohne Weiteres aufgebracht werden kann. Die relevanten Daten werden in unterschiedlichen zentralisierten Informationssystemen gespeichert, die jedoch keine nahtlosen Möglichkeiten für den Datenaustausch bieten. Diese zentralisierten Systeme haben sich als unzureichend erwiesen, um die erforderliche Transparenz und Effizienz im Zertifizierungsprozess zu gewährleisten.

Auf der Ebene der Europäischen Union existiert gegenwärtig keine verlässliche und umfassende Online-Trusted-Third-Party, die eine durchgängige und transparente Überwachung der Zertifizierungsprozesse gewährleisten könnte. Die aktuellen manuellen und zeitaufwendigen Prüfverfahren, einschließlich der manuellen Validierung von Zertifikaten, haben zu einer komplexen und oft undurchsichtigen Datenlandschaft geführt. Diese

Struktur ist anfällig für Betrug und Fehler, was die Integrität des gesamten Systems gefährdet. Die Notwendigkeit, diese Probleme zu beheben, erfordert einen erheblichen bürokratischen Aufwand, der viele Biogasanlagenbetreiber vor große Herausforderungen stellt. Diese Schwierigkeiten können dazu führen, dass Betreiber den aktuellen regulatorischen Verpflichtungen nicht vollständig nachkommen, was wiederum in Verbindung mit den gesunkenen EEG-Einspeisevergütungen dazu führt, dass immer mehr Betreiber gezwungen sind, ihre Anlagen zu schließen.

Angesichts dieser umfassenden Herausforderungen haben wir, gemeinsam mit unseren assoziierten Partnern, die sowohl politische als auch wirtschaftliche Akteure der Biomasse-Wertschöpfungskette repräsentieren, die Dringlichkeit der Situation erkannt. Um den bestehenden Defiziten im Zertifizierungsprozess entgegenzuwirken, bieten wir eine innovative und wettbewerbsfähige Lösung in Form des Blockchain-basierten Biomassennachweises Minimum Viable Product (BBBio-MVP) an. Diese Lösung zielt darauf ab, die bestehenden Probleme durch den Einsatz fortschrittlicher Technologien wie der Blockchain zu adressieren und eine umfassende, transparente und effiziente Methode zur Verwaltung und Überwachung der Biomassezertifizierung zu schaffen.

3. Neuartigkeit von BBBio

BBBio-MVP eliminiert die Nachteile des im vorherigen Abschnitt beschriebenen Prozesses. Ein erstes mögliches Prozessschaubild bzw. Architektur der Lösung könnte wie in Abbildung 2 aussehen.

In Anbetracht des Charakters des Biomassezertifizierungssystems gibt es zwei wesentliche Aspekte, die einer zentralen Architektur von BBBio-MVP entgegenstehen: Erstens ist die Biomasse-Wertschöpfungskette ein komplexes System, an dem viele Akteure beteiligt sind, die unterschiedliche Ansichten über den Stand der Zertifizierung von Biomasse haben; Biogasanlagenbetreiber wollen Biogas möglichst gewinnbringend verkaufen, während die Nutzer eine gute Qualität, eine sichere Versorgung und die Einhaltung ihrer Emissionsberichtspflichten benötigen. Zweitens wollen die Regulierungsbehörden die Biogasproduktion Bottom-up fördern und zugleich die Umweltfreundlichkeit des Biogases auf dem Markt sicherstellen. Die Europäische Union ist die grundlegende Instanz für die Festlegung der Regeln für die Zertifizierung; allerdings unterscheiden sich die Zertifizierungssysteme und Zertifizierungsstellen, die die Ausstellung und Übertragung kontrollieren, von Land zu Land. Je nach Land hat eine ausstellende Behörde das Recht, dem System Blöcke hinzuzufügen, während die Akteure der Biomasse-Wertschöpfungskette die Transaktionen lesen können, um die Herkunft der Biomasse zu überprüfen. Darüber hinaus können Gasnetzbetreiber (Distribution System Operators (DSOs) als zusätzliche Überprüfungsinstanz fungieren, und die nationalen Register können mit einer aktualisierten Version des Ledgers gekoppelt werden, um die Interoperabilität zwischen den Mitgliedstaaten der Europäischen Union zu verbessern.

Die asymmetrische Natur der Biogaswirtschaft passt zur dezentralen Natur der Blockchain. Die Gestaltung der Blockchain-IoT-Architektur basiert auf einer fundierten

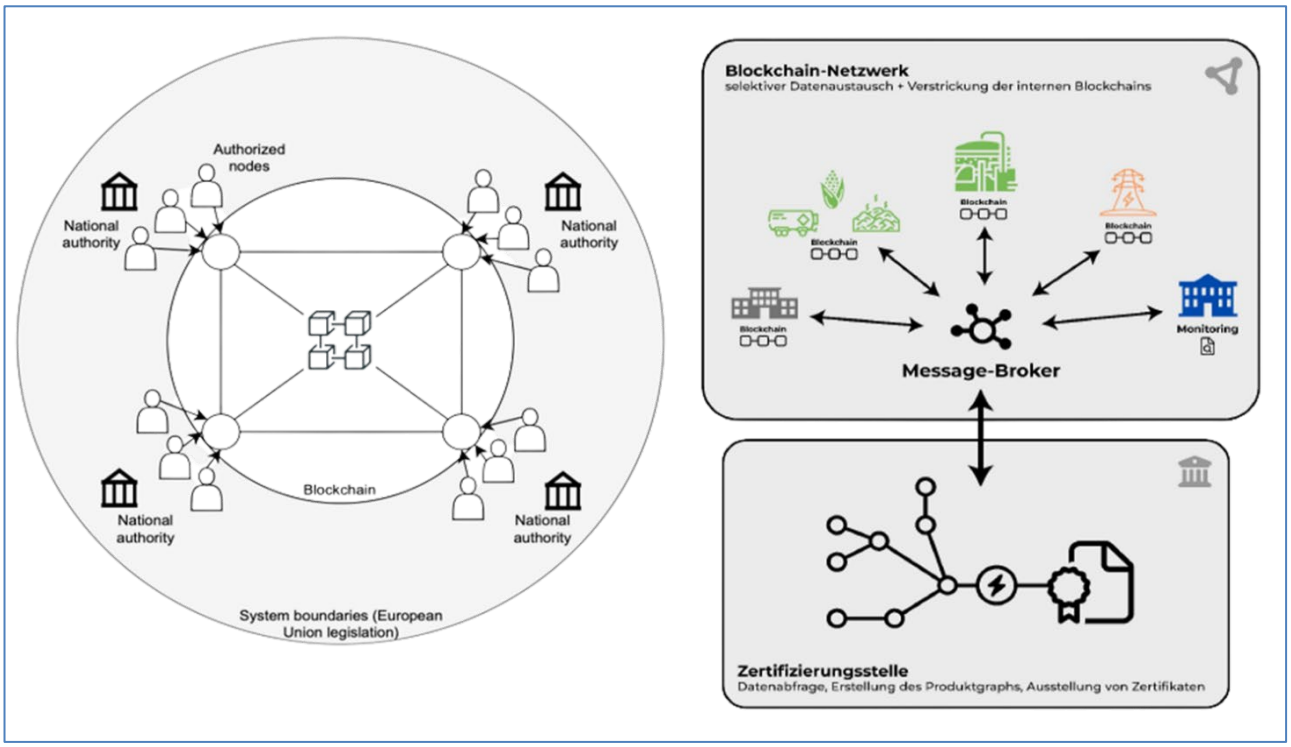

Abbildung 2: Architekturansatz für BBBio-MVP (Eigene Darstellung)

Analyse einschlägiger wissenschaftlicher Literatur und den daraus resultierenden Forschungsergebnissen [4, 5, 6,7]. Föderal- oder konsortial -verwaltete Blockchains bieten sich am besten für diesen Anwendungsfall an. Die Wahl der Konsortialarchitektur ist in Abbildung 2 gegeben. Je Mitgliedstaat kontrolliert eine nationale Behörde die spezifischen Regeln des Konsortiums und die akkreditierten autorisierten Nodes (Zertifizierungsstellen), die die Daten in das Blockchain-Netzwerk einspeisen. Für jeden Informationsfluss vom Wirtschaftsakteur zur Prüfbehörde kann ein privater Informationskanal eingerichtet werden, um die Vertraulichkeit des Wirtschaftsakteurs zu wahren. Die für die Zertifizierung relevanten Daten werden via ZKP abgefragt. Somit bleiben die Intellectual Properties (IPs) der Wirtschaftsakteure geschützt und es werden nur RED II-Vorgaben, wie die Offenbarung des CO2-Fußabdrucks, offengelegt. Die Zertifikate und Emissionsdaten werden anschließend im Kanal des Konsortiums enthüllt. Auf diese Weise können die regulatorischen Vorschriften eingehalten und ein europäisches Biomassezertifizierungsnetz ermöglicht werden. Ähnlich wie herkömmliche Datenbanken ist auch unsere Lösung kein Allheilmittel für fehlerhafte oder manipulierte externe Daten, die beispielsweise automatisch über IoT-Geräte in das System gelangen (bekannt als Oracle-Problem). Dennoch bietet unsere Lösung aufgrund ihres integrierenden, verknüpften Datenaustauschs zwischen verschiedenen Informationssystemen nicht nur Einblicke und Transparenz in Bezug auf die Rückverfolgbarkeit dessen, wer möglicherweise welche Manipulationen vorgenommen haben könnte, sondern ermöglicht auch effektiv die Verhinderung von Double-Spending (d.h. eine Verhinderung, dass dieselbe Zertifikatskopie mehrmals verwendet wird, obwohl sie nur einmal gültig sein sollte).

4. Umsetzungsmethode

Im Rahmen der Implementierung einer Blockchain-basierten Lösung für die Verwaltung und Nachverfolgung von Biomassenachweisen wird ein methodischer Ansatz verfolgt, der eine detaillierte und systematische Herangehensweise sicherstellt. Die folgende Darstellung skizziert die geplanten Schritte zur Realisierung dieses Projekts, wobei jeder Schritt eine präzise und differenzierte Betrachtung der Anforderungen, Technologien und Prozesse umfasst.

a) Evaluierung der Designanforderungen: Die erste Phase des Projekts besteht in der umfassenden Analyse und Bewertung der spezifischen Anforderungen und Kriterien, die an das Design der Lösung gestellt werden. Dieser Schritt ist von zentraler Bedeutung, um sicherzustellen, dass alle funktionalen und nicht-funktionalen Anforderungen präzise erfasst und dokumentiert werden. Die funktionalen Anforderungen umfassen die spezifischen Aufgaben, die das System erfüllen muss, wie die Erfassung, Speicherung und Überprüfung von Biomassenachweisen. Nicht-funktionale Anforderungen betreffen Aspekte wie Systemperformance, Benutzerfreundlichkeit, Sicherheit und Skalierbarkeit. Eine detaillierte Anforderungsanalyse ermöglicht es, ein Design zu entwickeln, das die Bedürfnisse aller relevanten Stakeholder adressiert und die Grundlage für die nachfolgenden Entwicklungsphasen bildet.

b) Evaluierung einer geeigneten Blockchain-Technologie: Im Anschluss an die Anforderungsanalyse erfolgt die Evaluierung und Auswahl der am besten geeigneten Blockchain-Technologie. Diese Phase beinhaltet eine gründliche Untersuchung der verfügbaren Blockchain-Plattformen hinsichtlich ihrer Sicherheitsmerkmale, Skalierbarkeit und Integrationsfähigkeit. Sicherheitsmerkmale sind entscheidend, um die Integrität und Vertraulichkeit der auf der Blockchain gespeicherten Daten zu gewährleisten. Die Skalierbarkeit der Technologie ist wichtig, um sicherzustellen, dass das System mit wachsender Nutzung und Datenmenge effektiv umgehen kann. Die Integrationsfähigkeit bezieht sich auf die Möglichkeit, die Blockchain-Lösung nahtlos in bestehende Systeme zu integrieren und mit anderen Technologien und Prozessen zu kombinieren.

c) Erstellung und Validierung eines geeigneten Smart Contract Formats: Ein wesentlicher Bestandteil der Blockchain-Lösung ist die Entwicklung und Prüfung eines Formats für Smart Contracts. Smart Contracts sind selbst ausführende Verträge, deren Bedingungen direkt in den Code geschrieben werden. Die Erstellung eines geeigneten Formats für Smart Contracts umfasst die Definition der Bedingungen und Regeln, die die Interaktionen zwischen den Beteiligten regeln. Die Validierung dieses Formats stellt sicher, dass die Smart Contracts alle relevanten Aspekte der Transaktionen und Interaktionen korrekt abbilden und zuverlässig ausgeführt werden. Diese Phase ist entscheidend für die effiziente und sichere Verwaltung der Biomassenachweise innerhalb der Blockchain.

d) Entwicklung eines Formats zur Abbildung von Biomassenachweisen: Die Konzeption und Implementierung eines Formats innerhalb der Blockchain zur präzisen und sicheren Abbildung und Verwaltung von Biomassenachweisen stellt einen weiteren wichtigen Schritt dar. Dieses Format muss den Anforderungen an Transparenz, Nachverfolgbarkeit und Integrität gerecht werden. Es beinhaltet die Entwicklung von Standards und Protokollen für die Speicherung und den Austausch von Biomassenachweisen auf der Blockchain, um eine klare und nachvollziehbare Dokumentation aller relevanten Informationen zu gewährleisten.

e) Entwicklung und Implementierung der Blockchain-Lösung: Die eigentliche Entwicklung und Integration der Blockchain-Plattform bildet den Kern des Projekts. Dies umfasst die vollständige Implementierung der Blockchain-Technologie sowie die Programmierung und Integration der Smart Contracts, die die Regeln und Bedingungen für die Verwaltung von Biomassenachweisen festlegen. In dieser Phase wird auch die Möglichkeit zur Hinterlegung und Verwaltung von Biomassenachweisen

innerhalb des Systems geschaffen. Die erfolgreiche Implementierung dieser Plattform ist entscheidend für die Funktionalität und Effektivität der gesamten Lösung.

f) Entwicklung geeigneter technischer Schnittstellen: Die Schaffung technischer Schnittstellen ist von zentraler Bedeutung, um eine nahtlose Integration der Blockchain-Lösung mit bestehenden Systemen der Nutzer zu ermöglichen. Diese Schnittstellen müssen so gestaltet werden, dass sie die Kommunikation zwischen der Blockchain-Plattform und anderen Systemen effizient und fehlerfrei ermöglichen. Zudem wird die Integration von IoT-Technologien in Betracht gezogen, um die Datenerfassung und -übertragung zu verbessern und eine automatische und präzise Erfassung von Biomassenachweisen zu ermöglichen.

g) Entwicklung geeigneter Datenformate: Für den Austausch prozessrelevanter Daten müssen standardisierte und kompatible Datenformate entwickelt werden. Diese Formate sind erforderlich, um eine effiziente und fehlerfreie Kommunikation zwischen den verschiedenen Systemen und Akteuren zu gewährleisten. Die Standardisierung der Datenformate ermöglicht eine konsistente und zuverlässige Verarbeitung der Informationen und trägt zur Vermeidung von Dateninkonsistenzen und -fehlern bei.

h) Schaffung der technischen und ökonomischen Grundlagen zur Gründung einer Betreibergesellschaft: Abschließend werden die technischen und ökonomischen Grundlagen für die Gründung einer Betreibergesellschaft geschaffen. Diese Gesellschaft wird für die langfristige Verwaltung und Weiterentwicklung der Blockchain-Lösung verantwortlich sein. Die Etablierung der notwendigen technischen Infrastruktur sowie der wirtschaftlichen Rahmenbedingungen ist entscheidend für den nachhaltigen Betrieb und die kontinuierliche Weiterentwicklung des Systems. Diese Phase beinhaltet die Sicherstellung der finanziellen Mittel, die Rekrutierung von Fachpersonal und die Implementierung von Geschäftsprozessen, die den langfristigen Erfolg der Betreibergesellschaft unterstützen.

Durch die systematische und detaillierte Umsetzung dieser Schritte wird sichergestellt, dass die Blockchain-basierte Lösung für die Biomassenachweise effektiv, sicher und zukunftsfähig ist.

5. Fazit

Die vorgestellte Methodik zur Umsetzung des „Blockchain-basierten Biomassenachweises“ (BBBio) bietet einen umfassenden und innovativen Ansatz zur Verbesserung der Biomassezertifizierung. Durch die Integration fortschrittlicher Technologien wie Blockchain, Smart Contracts, IoT und Zero-Knowledge-Proofs wird nicht nur die Effizienz gesteigert, sondern auch die Transparenz und Rückverfolgbarkeit in der gesamten Wertschöpfungskette der Biogasproduktion erheblich verbessert. Die sorgfältige Evaluierung und Implementierung der jeweiligen Komponenten garantieren eine robuste und praxisorientierte Lösung, die sowohl den aktuellen regulatorischen Anforderungen als auch den Bedürfnissen der Stakeholder gerecht wird. Das BBBio-MVP stellt einen wesentlichen Fortschritt dar, indem es komplexe bürokratische Prozesse durch automatisierte und digitale Abläufe ersetzt, was zu einer signifikanten Reduzierung von Verwaltungsaufwand und Fehleranfälligkeit führt. Die Schaffung neuer Arbeitsplätze, die Förderung der regionalen Wirtschaft und die Stärkung des Wissenstransfers zwischen Forschung und Industrie sind bedeutende Vorteile, die das Vorhaben mit sich bringt. Zudem trägt die Entwicklung von Standardisierten Datenformaten und technischen Schnittstellen zur nahtlosen Integration mit bestehenden Systemen bei, wodurch eine effektive und nachhaltige Umsetzung sichergestellt wird. Insgesamt stellt das BBBio einen bedeutenden Schritt in der Weiterentwicklung der Biomassezertifizierung dar und positioniert sich als wegweisender Ansatz im Bereich der nachhaltigen Energieversorgung. Die Etablierung einer Betreibergesellschaft und die Förderung von Forschungs- und Entwicklungsaktivitäten unterstreichen die langfristigen Ziele und die strategische Bedeutung dieses Vorhabens. Durch diese umfassende Methodik wird nicht nur die technische Machbarkeit gewährleistet, sondern auch die Grundlage für eine nachhaltige und zukunftsfähige Biomassezertifizierung geschaffen.

Literaturverzeichnis

[1] Eur-Lex (2023). RICHTLINIE (EU) 2018/2001 DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Förderung der Nutzung von Energie aus erneuerbaren Quellen, unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32018L2001&qid=1703054246771 (abgerufen am 20.12.2023)

[2] Eur-Lex (2023). RICHTLINIE 2009/28/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES, unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:140:0016:0062:de:PDF (abgerufen am 20.12.2023).

[3] BLE (2023). Nabisy - Nachhaltige-Biomasse-System, unter: https://nabisy.ble.de/app/start (abgerufen am 20.12.2023)

[4] Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A Survey on blockchain for industrial Internet of Things. Alexandria Engineering Journal, 61(8), 6001–6022. https://doi.org/10.1016/j.aej.2021.11.023

[5] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), 243–252. https://doi.org/10.1109/ICSA.2017.33

[6] Sedlmeir, J., Völter, F., & Strüker, J. (2021). The next stage of green electricity labeling: Using zero-knowledge proofs for blockchain-based certificates of origin and use. ACM SIGEnergy Energy Informatics Review, 1(1), 20–31. https://doi.org/10.1145/3508467.3508470

[7] Elisa, N., Yang, L., Li, H., Chao, F., & Naik, N. (2019). Consortium Blockchain for Security and Privacy-Preserving in E-government Systems.

Flex-Smart-DP: Application of Blockchain Technology for Dynamic Pricing and Flexible Access in Sports and Tourism

Jan Lippert, Volker Wannack
Hochschule Mittweida, Mittweida, Deutschland

This paper explores the theoretical application of blockchain technology for dynamic pricing and flexible access management in the sports and tourism industries. Focusing on the proposed FlexSmart-DP project, this research examines the theoretical deployment of smart contracts and tokenization as a means of optimizing resource use, enhancing operational efficiency, and ensuring regulatory compliance. Additionally, the paper discusses the technical, legal, and economic challenges that could arise during the implementation of blockchain in these sectors, proposing potential solutions based on the latest advancements in blockchain technology.

In diesem Paper wird die theoretische Anwendung der Blockchain-Technologie für dynamische Preisgestaltung und flexibles Zugangsmanagement in der Sport- und Tourismusbranche untersucht. Mit dem Schwerpunkt auf dem vorgeschlagenen Flex-Smart-DP-Projekt wird der theoretische Einsatz von Smart Contracts und Tokenisierung als Mittel zur Optimierung der Ressourcennutzung, zur Verbesserung der betriebswirtschaftlichen Effizienz und zur Gewährleistung der Einhaltung gesetzlicher Vorschriften untersucht. Darüber hinaus erörtert das Papier die technischen, rechtlichen und wirtschaftlichen Herausforderungen, die bei der Implementierung von Blockchain in diesen Sektoren auftreten könnten, und schlägt potenzielle Lösungen vor, die auf den neuesten Fortschritten der Blockchain-Technologie basieren.

1. Introduction

1.1 Context and Motivation

Blockchain technology, initially developed as the backbone for cryptocurrencies, has evolved to offer various possibilities for multiple sectors, ranging from finance to supply chain management. Blockchain's inherent properties of transparency, security, and decentralization position it as a transformative technology, particularly for industries such as sports and tourism, which deal with highly variable demand and complex access management. Recent studies have shown that blockchain can enhance trust and transparency in sectors like sports, where it is used for ticket sales and fan engagement (Rashideh, 2020; Blockchain Use Cases in Sports Industry, 2024)

This paper presents the theoretical framework for the FlexSmart-DP project, a future initiative aimed at exploring the use of blockchain technology for managing dynamic pricing and access control in sports and tourism facilities. The project proposes to apply smart contracts and tokenized access rights to enhance efficiency, flexibility, and security in these industries. Although the FlexSmart-DP project is currently at the conceptual stage, this paper outlines how blockchain technology could be utilized in this context and examines the potential challenges and benefits of its implementation.

1.2 Objectives of the Study

The goal of this paper is to provide a theoretical examination of the following:

- How blockchain technology could be applied to dynamic pricing and access control in sports and tourism within the FlexSmart-DP project.
- The possible architecture and design of the blockchain-based system.
- The legal and regulatory challenges that may arise during the implementation of blockchain in these sectors.
- The potential for future scalability and expansion of blockchain applications in sports and tourism.

2. Literature Review

2.1 Blockchain and Smart Contracts: Concepts and Applications

Blockchain, a decentralized and immutable ledger, allows for the secure recording of transactions across a distributed network. Its key features, such as transparency and resistance to tampering, have led to its adoption in sectors beyond cryptocurrencies, including healthcare, finance, and logistics (Nakamoto, 2008). Smart contracts, which are self-executing agreements encoded on the blockchain, have been proposed as a solution for automating processes and ensuring that transactions occur according to predetermined conditions (Buterin, 2014). Additionally, blockchain's potential to enable disintermediation by removing intermediaries like online travel agents and brokers can significantly reduce costs and improve the user experience (Valeri & Baggio, 2021; Rashideh, 2020).

Although the application of smart contracts in dynamic pricing and access management is still in its infancy, recent developments suggest that they have the potential to disrupt traditional systems by reducing intermediaries and increasing trust between parties (Di Angelo & Salzer, 2020). This paper builds on existing research by proposing a theoretical application of smart contracts in the FlexSmart-DP project for managing sports and tourism services.

2.2 Dynamic Pricing: A Theoretical Approach

Dynamic pricing is a practice that adjusts prices based on market conditions, demand, and other variables. It has been successfully implemented in industries such as airlines and hospitality, where prices are continuously updated based on factors like customer demand, availability, and timing (Wang et al., 2019). Recent blockchain research in the sports industry shows that dynamic pricing can be implemented transparently and securely using smart contracts (Blockchain Use Cases in Sports Industry, 2024)

In the sports and tourism industries, dynamic pricing presents an opportunity to better align pricing strategies with market conditions. The FlexSmart-DP project proposes the use of smart contracts to manage dynamic pricing in real-time, with blockchain ensuring that all price changes are transparent and fair. This would allow for the automated adjustment of prices based on variables such as event popularity, ticket demand, and weather conditions, theoretically resulting in more efficient resource use and increased revenue.

2.3 Tokenization of Access Rights: Conceptual Framework

Tokenization refers to the process of representing ownership or access rights over an asset through digital tokens recorded on a blockchain. These tokens are immutable, secure, and can be easily transferred or traded without intermediaries. Tokenization has been proposed as a way to manage ownership of physical and digital assets in fields like real estate, art, and intellectual property (Gunnarsson et al., 2020).

The proposed FlexSmart-DP project envisions a system where access to sports and tourism facilities is managed through tokenized rights. For example, a token could represent a ticket to a sports event or a day pass to a museum. These tokens could be stored in digital wallets and traded on a decentralized marketplace. Blockchain-enabled virtual reality experiences, such as those developed by Victoria VR, have shown how blockchain-backed tokenization can enhance customer experiences in the tourism sector by offering secure access to digital and physical experiences (McKercher & Prideaux, 2024).

3. Methodology

3.1 Theoretical Approach to the FlexSmart-DP Project

The FlexSmart-DP project, as proposed, seeks to apply blockchain technology to the sports and tourism industries in a way that maximizes efficiency and minimizes administrative overhead. This section outlines the theoretical structure of the project, including the design of smart contracts for dynamic pricing and the implementation of tokenized access rights. The methodology presented is intended as a conceptual framework for future implementation.

3.2 Conceptual System Design

The proposed system for FlexSmart-DP would be built on a decentralized blockchain platform, likely leveraging the Ethereum blockchain for its robust smart contract capabilities (Buterin, 2014). The system would consist of several key components:

- Smart Contracts for Pricing: Algorithms embedded in smart contracts would automatically adjust prices in real-time based on demand, availability, and other factors. These smart contracts would be coded with predefined rules governing price changes and would operate independently of human intervention. Similar systems are already in place in tourism, where blockchain-enabled automation is streamlining operations such as flight delay insurance and secure hotel check-ins (Erceg et al., 2020; Nam et al., 2024)
- Tokenized Access Rights: Access to facilities and services would be represented by digital tokens stored on the blockchain. Users could purchase, trade, or redeem these tokens using a digital wallet, and all transactions would be recorded on the blockchain to ensure security and transparency.

4. Blockchain for Dynamic Pricing and Tokenized Access

4.1 Smart Contracts for Dynamic Pricing: A Theoretical Framework

In the FlexSmart-DP project, smart contracts are proposed as the central mechanism for managing dynamic pricing. These contracts would be pre-programmed with algorithms that respond to variables such as customer demand, time of day, or external events like weather changes or special promotions. For example, the price of a ticket to a sporting event might increase as demand rises in the days leading up to the event, while prices for hotel stays might decrease during periods of low occupancy.

The use of blockchain ensures that all price changes are publicly recorded and verifiable, promoting transparency and trust among users. In a future scenario, facility operators would have the ability to customize the rules

governing pricing, ensuring that their specific needs are met.

4.2 Tokenization of Access Rights: Conceptual Application

The proposed FlexSmart-DP project envisions a system where access rights to facilities and services are represented by digital tokens. Each token would represent the right to access a specific service, such as entry to a sports event or a pass to a tourist attraction. The tokenization process ensures that access rights are securely recorded on the blockchain, making them tamper-proof and easily transferable. This system would provide users with greater flexibility, as they could buy, sell, or trade their access tokens on a decentralized marketplace.

5. Legal and Compliance Considerations

5.1 Regulatory Frameworks for Blockchain in Sports and Tourism

The implementation of blockchain technology in regulated industries such as sports and tourism will require careful consideration of existing legal and regulatory frameworks. The proposed FlexSmart-DP project must comply with relevant laws, such as the Markets in Crypto-Assets Regulation (MiCA) in the European Union, which governs the issuance and management of cryptocurrencies and tokenized assets (Schütte et al., 2018).

Blockchain adoption in tourism has also been met with regulatory challenges, particularly concerning data privacy and the legal status of tokenized assets (Önder & Treiblmaier, 2018). As the project moves forward, it will need to navigate this complex regulatory landscape to ensure that it complies with relevant laws while maximizing the benefits of blockchain technology.

6. Potential Challenges and Limitations

6.1 Scalability and Integration Issues

While the theoretical framework for the FlexSmart-DP project offers significant potential, several challenges must be considered before full-scale implementation. One of the primary concerns is scalability. Blockchain networks, particularly public blockchains like Ethereum, have known limitations when it comes to processing large volumes of transactions quickly. High-traffic periods during major sports events or tourist seasons could overwhelm the network, resulting in delays or higher transaction costs due to congestion (Nam et al., 2019; McKercher & Prideaux, 2024).

To mitigate this risk, layer-2 scaling solutions, such as sidechains or state channels, could be explored. These solutions allow transactions to be processed off-chain while still benefiting from the security and decentralization of the main blockchain network (Stojmenova Duh et al., 2019). Additionally, adopting permissioned blockchains, which are partially decentralized and involve pre-authorized participants, might offer more control over scalability while ensuring operational efficiency (Rashideh, 2020).

6.2 Legal Uncertainty and Evolving Regulations

Blockchain technology is still developing within a rapidly evolving regulatory landscape. Laws and regulations concerning blockchain, cryptocurrencies, and tokenized assets differ across jurisdictions and are subject to change. One of the challenges the FlexSmart-DP project will face is ensuring compliance with both local and international regulations while also adapting to legal changes. The Markets in Crypto-Assets Regulation (MiCA), for instance, provides a robust framework for cryptocurrency use in the EU but might require ongoing adaptation as new rules emerge (Önder & Treiblmaier, 2018).

There are also concerns regarding data privacy, particularly with regard to regulations like the General Data Protection Regulation (GDPR) in the European Union. The immutable nature of blockchain conflicts with GDPR's requirement for data to be alterable or deletable upon request. To address this issue, the FlexSmart-DP project could explore solutions like zero-knowledge proofs and encryption techniques to ensure that personal data is stored securely while remaining compliant with GDPR (Valeri & Baggio, 2021).

6.3 User Adoption and Education

Blockchain technology is still relatively new to the mainstream public. User adoption could present a significant challenge as many individuals may not be familiar with how to interact with blockchain-based systems, particularly when it comes to managing digital wallets, trading tokenized assets, and utilizing smart contracts. Effective user education and training programs will be key to ensuring the success of the FlexSmart-DP project (Nam et al., 2019). This includes educating both consumers and service providers about the benefits of blockchain while also providing them with the tools and resources to engage confidently with the technology (Blockchain in Sports, 2024).

Moreover, the project will need to consider user experience design to ensure that the blockchain system is easy to navigate. For example, digital wallets and platforms for trading access tokens should have intuitive interfaces to reduce the complexity of blockchain interactions, thereby encouraging broader adoption among non-technical users.

6.4 Technological Limitations and Costs

While blockchain technology offers many advantages, its implementation is not without costs. The energy consumption associated with certain consensus mechanisms, such as Proof of Work, raises concerns about sustainability, especially as environmental regulations become more stringent. Exploring more energy-efficient consensus algorithms, such as Proof of Stake or Proof of Authority, could help mitigate the environmental impact

of the blockchain network used in the FlexSmart-DP project (Erceg et al., 2020; Nam et al., 2024).

Additionally, the initial investment in infrastructure will be substantial, particularly for smaller organizations in the sports and tourism sectors. Upgrading legacy systems, integrating blockchain with existing databases, and ensuring compatibility with IoT devices will require significant resources, both financial and technical. These upfront costs must be weighed against the potential long-term benefits of blockchain implementation, such as reduced fraud, lower administrative costs, and improved operational efficiency.

7. Conclusion and Future Directions

7.1 Conclusion

The FlexSmart-DP project presents a promising theoretical framework for the application of blockchain technology in the sports and tourism industries. By leveraging smart contracts for dynamic pricing and tokenized access rights, the project could provide significant benefits in terms of operational efficiency, security, and transparency. However, several challenges remain, particularly in the areas of scalability, legal compliance, and user adoption. The project will need to carefully navigate these challenges to ensure its successful implementation.

The proposed system's ability to enhance trust and transparency through blockchain's decentralized architecture offers a distinct competitive advantage for sports and tourism operators. These industries can benefit from automated processes and reduced reliance on intermediaries, leading to more efficient operations and improved customer experiences (Rashideh, 2020; Blockchain in Sports, 2024).

7.2 Future Work

Future work will focus on further refining the proposed system architecture and exploring solutions to the challenges identified in this paper. This includes researching scaling solutions for blockchain networks, developing compliance strategies for evolving regulations, and designing educational programs to increase user adoption.

As blockchain technology continues to evolve, the potential for expanding its use in other aspects of the sports and tourism industries is vast. Future research could explore the application of blockchain in loyalty programs, insurance automation, and event management, where the benefits of decentralized systems and smart contracts could further enhance the efficiency and security of operations (Önder & Treiblmaier, 2018). As the FlexSmart-DP project progresses, it could serve as a model for future blockchain-based innovations in these sectors..

References

[1] Blockchain Use Cases in the Sports Industry (2024). International Journal of Networked and Distributed Computing.

[2] Erceg, V., et al. (2020). The impact of blockchain on tourism: Automation, security, and trust. Information Technology & Tourism.

[3] McKercher, B., Prideaux, B. (2024). Blockchain and tourism: Implications for the future. Journal of Hospitality and Tourism.

[4] Nam, K., Dutt, S.C., Chathoth, P., Khan, S.M. (2019). Blockchain technology for smart cities and smart tourism: Latest trends and challenges. Journal of Asia-Pacific Tourism Research.

[5] Rashideh, W. (2020). Blockchain technology framework: Current and future perspectives for the tourism industry. Tourism Management.

[6] Stojmenova Duh, E., et al. (2019). Cryptoeconomic incentives in academic publishing: A case study. Journal of Cryptoeconomics.

[7] Valeri, M., & Baggio, R. (2021). Blockchain and the tourism value chain: Disintermediation, data privacy, and consumer empowerment. Information Technology & Tourism.

[8] Önder, I., Treiblmaier, H. (2018). Blockchain and tourism: Three research propositions. Annals of Tourism Research.

ISSN 1437-7624