Babel *et al. Energy Informatics* 2022, **5**(Suppl 1):27
https://doi.org/10.1186/s42162-022-00199-3

Energy Informatics

RESEARCH Open Access

Enabling end-to-end digital carbon emission tracing with shielded NFTs

Matthias Babel[1,2], Vincent Gramlich[1,2], Marc-Fabian Körner[1,2*], Johannes Sedlmeir[1,2], Jens Strüker[1,2] and Till Zwede[1,2]

From The 11th DACH+ Conference on Energy Informatics 2022
Freiburg, Germany. 15-16 September 2022

*Correspondence:
marc.koerner@fim-rc.de

[1] FIM Research Center, University of Bayreuth, Wittelsbacherring 10, 95447 Bayreuth, Germany
[2] Branch Business and Information Systems Engineering of Fraunhofer FIT, Wittelsbacherring 10, 95447 Bayreuth, Germany

Abstract

In the energy transition, there is an urgent need for decreasing overall carbon emissions. Against this background, the purposeful and verifiable tracing of emissions in the energy system is a crucial key element for promoting the deep decarbonization towards a net zero emission economy with a market-based approach. Such an effective tracing system requires end-to-end information flows that link carbon sources and sinks while keeping end consumers' and businesses' sensitive data confidential. In this paper, we illustrate how non-fungible tokens with fractional ownership can help to enable such a system, and how zero-knowledge proofs can address the related privacy issues associated with the fine-granular recording of stakeholders' emission data. Thus, we contribute to designing a carbon emission tracing system that satisfies verifiability, distinguishability, fractional ownership, and privacy requirements. We implement a proof-of-concept for our approach and discuss its advantages compared to alternative centralized or decentralized architectures that have been proposed in the past. Based on a technical, data privacy, and economic analysis, we conclude that our approach is a more suitable technical backbone for end-to-end digital carbon emission tracing than previously suggested solutions.

Keywords: Blockchain, Certificate, Decarbonization, Distributed ledger technology, Electric vehicle, Guarantee of origin, Personal carbon tracing, Privacy, Non-fungible token, Sustainability, Zero-knowledge proof

Introduction

Tackling the climate crisis is now arguably one of the most pressing tasks for business, politics, and society. Against this background, various stakeholders are highly engaged to promote the necessary deep decarbonization (United Nations Security Council 2021). Corresponding attempts of the energy transition aim at decreasing the Greenhouse Gas (GHG) emissions associated with energy systems worldwide, including generation, transmission, and consumption (IPCC 2021, United Nations 2015). To effectively reduce GHG and above all CO_2 emissions, both companies and end consumers must

be empowered and incentivized to act in a CO_2-adaptive manner (Strüker et al. 2021). Consequently, there is a need for verifiable, fine-granular carbon accounting that allows these stakeholders to access corresponding information on CO_2 emissions of their own processes, as well as goods and services that they purchase and to comprehensively disclose it to stakeholders and legislators (Financial Times 2021, Sullivan and Gouldson 2012; Heffron 2021; Strüker et al. 2021).

However, to date such fine-granular and verifiable data is typically not available (Sedlmeir et al. 2021). For instance, companies that participate in the European Union Emissions Trading System (EU-ETS) are only required to compile and submit their corresponding CO_2 reporting once a year (European Commission 2021). Disclosure also only happens ex-post. This means that the temporal granularity of the data on CO_2 emissions is too low to incentivize adaptive behavior. Moreover, the European Guarantees of Origin (GOs) and EU-ETS certificates represent large quantities of Megawatt hours (MWHs) of electricity and tons of CO_2 (Watanabe and Robinson 2005, Association of Issuing Bodies 2021), thus, lacking the resolution to include smaller stakeholders in CO_2 -adaptive decisions.

Additionally, the current reporting process involves the manual collection and inspection of data and offers no support for automatic verification, scaling the granularity of the current approach is arguably not practical. Consequently, neither the CO_2-adaptive control of business processes or consumption decisions is possible with the current approach, nor can stakeholders provide evidence for their own or their products' carbon footprints. Our research starts exactly at this point and aims to provide a concept that enables an end-to-end tracing system where CO_2 emission data is verifiable by end consumers, leveraging innovative emerging digital technologies in order to make the energy transition a success. For emission trading and related areas like electricity labeling, several studies have highlighted the suitability of digital platforms to record related information. Researchers have specifically proposed blockchain-based solutions, with their ability to provide cryptographic verifiability and to unite different stakeholders on a single neutral data sharing platform (Sedlmeir et al. 2021; Al Sadawi et al. 2021; Albrecht et al. 2018; Knirsch et al. 2020; Castellanos et al. 2017; Richard et al. 2019; Djamali et al. 2021). However, such proposals generally face significant privacy and trust challenges: In a centralized system, the platform owner would not only need to be trusted regarding data availability and integrity. It also would have significant market power through its control of the platform and access to sensitive personal and business relevant data in terms of energy procurement and emissions labeling (Körner et al. 2022). For blockchain-based approaches, the trust issues disappear, but the replicated data storage and processing as well as the impracticality of deleting data from the ledger aggravates issues with sensitive information and conflicts with regulation such as the General Data Protection Regulation (GDPR) (Al Sadawi et al. 2021; Zhang et al. 2019; Munilla Garrido et al. 2021; Sedlmeir et al. 2022).

Several architectures proposed by related work, such as Al Sadawi et al. (2021), represent carbon emissions as tokens on a blockchain. The corresponding architectures are different, for instance, regarding the choice of a public or private blockchain and their consensus mechanism, which can have significant impact on their scalability, energy consumption, and the extent to which sensitive information is problematic (Beck et al.

2018; Cachin and Vukolić 2022; Sedlmeir et al. 2020). Specifically, there is often general criticism that blockchain technology is energy intensive by design; yet, this only holds true for public blockchains that use Proof of Work (PoW) as consensus mechanism. In contrast, energy consumption is not an issue for public blockchains with other consensus mechanisms, such as Proof of Stake (PoS), or permissioned blockchains with voting-based consensus (Sedlmeir et al. 2020; Rieger et al. 2022; Gola and Sedlmeir 2022). Another dimension for comparing such proposals is whether the carbon emission tokens are non-distinguishable (fungible) or distinguishable (non-fungible). Most of the related work focuses on non-fungibility since it enables the traceability and verifiability of CO_2 tokens according to their origin, but the uniqueness of the tokens and transactions increases the ability to attribute stakeholders to their pseudonymous wallet addresses on a public blockchain ledger and is, hence, problematic both from the perspective of organizations and individuals (Sedlmeir et al. 2022; Biryukov et al. 2014; Schellinger et al. 2022). On the other hand, privacy-oriented, blockchain-based solutions, such as Sasson et al. (2014), or solutions that adapt similar approaches in energy-related use cases (Baza et al. 2021), require that tokens are indistinguishable (fungible) to make transactions unlinkable (Pfitzmann and Hansen 2010), compromising the ability to trace and differentiate different emission sources or to hold stakeholders accountable for malicious behaviour.

Thus, we observe an apparent tradeoff between the verifiability and traceability of tokenized CO_2 credits on the one side and the protection of sensitive information on the other side. We aim to align these requirements by using a fundamentally new approach: This paper proposes a solution that combines shielded, fractional Non-Fungible Tokens (NFTs) with off-chain, bilateral data exchange to provide verifiable CO_2 emission information along electricity supply chains—with high temporal and quantitative resolution to enable CO_2-adaptive decision making, while keeping sensitive information confidential. Our approach is *blockchain-agnostic*: as we keep sensitive information off the ledger, we do not need to consider the above-mentioned aggravated confidentiality issues in public blockchains anymore. Depending on the required guarantees in terms of integrity and availability, and stakeholders' reservations in terms of market power of a platform owner, the system can then be built on top of a centralized or decentralized ledger.

Our paper is structured as follows: In the "Background and related work" section, we give a detailed overview of related research and previous work on documenting carbon emissions. Next, we shed light on our technical architecture in the "Implementation" section and describe how we use our approach in the exemplary "Application for the case of charging electric vehicles" section. We then evaluate the practicality and solution fitness of our approach in the Contribution and Discussion section where we also discuss the wide-ranging contribution of our approach. Finally, we summarize our findings in the "Conclusion".

Background and related work

Research stream on energy informatics and CO_2 emission tracing

The research stream on Energy Informatics shares large thematic overlaps with the Green Information Systems (IS) research area (Watson et al. 2010; vom Brocke et al. 2013) and is considered to be highly interdisciplinary (Staudt et al. 2019). Its area of

applications is widespread, ranging, among others, from topics concerning energy efficiency (Watson et al. 2010), energy flexibility, e.g., provided by electric vehicles (Holly et al. 2020) or its exploitation via artificial intelligence (Fridgen et al. 2022; Hanny et al. 2022), over data centers that are enabled to act in the sense of the energy transition (Klingert 2018; Fridgen et al. 2021), to the potential of IS for future energy data spaces to improve collaboration and energy systems' robustness (Körner et al. 2022). In 2014, Goebel et al. provided an overview of goals, themes, and use cases of Energy Informatics research that distinguishes relevant topics between "smart energy-saving systems" and "smart grids" (Goebel et al. 2014). More recently, several papers from the Energy Informatics community have emphasized the urgent relevance of decreasing CO_2 emissions by appropriate IS (Fiorini and Aiello 2018; de Lima et al. 2021; Zampou et al. 2022).

Against this background, Energy Informatics scholars are encouraged to elaborate on comprehensive and scalable digital solutions that are capable of providing CO_2 data in adequate granularity in order to enable a purposeful CO_2-adaptive decision making. Related work has already argued that there is a need for higher temporal as well as spatial granularity of CO_2 in energy management and in energy markets (Strüker et al. 2021; Pina et al. 2012). To enable CO_2-adaptive actions, corresponding CO_2 emissions must be easy to disclose along products' life cycles and supply chains to allow for the differentiation of low-carbon businesses and products (Sedlmeir et al. 2021, World Economic Forum 2021). This can even help businesses become more competitive, as consumers are increasingly willing to pay for sustainable products, reinforcing the transition towards sustainable production (Herbes and Ramme 2014; Goebel et al. 2018). The adoption of Personal Carbon Allowances (PCAs) may further accelerate this trend by turning CO_2 -adaptive decision making into a necessity for businesses and end-consumers alike (Fuso Nerini et al. 2021). However, measuring environmental performance adequately is challenging due to limited data availability (Strüker et al. 2021; Björklund et al. 2012), complex supply chain networks—ranging from player diversity to inadequacy of current supply chain metrics—and corresponding enterprise systems (Hervani et al. 2005; Ahi and Searcy 2015; Lehtinen and Ahola 2010).

Moreover, specifically the fine-granular recording of CO_2 emissions across different suppliers within or even across sectors is not only challenging to implement and govern but also raises substantial data confidentiality concerns (Hassini et al. 2012). Furthermore, when a corresponding centralized platform needs to be provided by a business or international organization, there will likely be issues regarding trust and economic or political power. On the other hand, solutions incorporated in organizations' Enterprise Resource Planning (ERP) systems lack interoperability and end-to-end verifiability owing to their fragmentation. Therefore, businesses and end-customers require specialized IS to capture and to analyze sustainability-related data along their supply chains (Maestrini et al. 2017; Qorri et al. 2018). Today, these IS should reveal information only selectively instead of providing complete transparency for all parties involved owing to the sensitivity of the respective fine-granular CO_2 emission data. Nonetheless, they must provide end-to-end traceability, starting from the consumer and pointing back to the corresponding sources, to enable the provisioning and levering of verifiable and fine-granular CO_2 emission data necessary to facilitate and incentivize CO_2-adaptive decision making.

As electricity systems are responsible for a large share of the global CO_2 emissions (Rouholamini et al. 2020), and they are at the same time arguably one of the simplest examples of a connected supply chain of a relatively homogeneous good, we focus on emissions from the generation of electricity. On the electricity market—among other things due to the growth of renewable energy sources—there is now some degree of differentiation according to the level of CO_2 intensity, so provenance is not a trivial topic (Sedlmeir et al. 2021). On the other hand, there are no repeated refinements or assemblies of goods that were themselves manufactured with some CO_2 footprint to a new product in a process that may is potentially carbon-intensive in itself. In addition, electricity data for industrial consumption and production is already generated in useful 15-min intervals within the synchronous grid of Central Europe (Märkle-Huß et al. 2018), and the provisioning of smart-meters aims to produce comparable data streams for small consumers in the foreseeable future, too (Zhou and Brown 2017). The tracking of CO_2 emissions along electricity supply chains is hence an appropriate and illustrative use-case that we will focus on in the following (cf. Application for the Case of Charging Electric Vehicles section). Against this background, our research contributes to Energy Informatics research and provides a novel concept on how to bring traceability regarding CO_2 emissions into electricity systems by appropriate IS solutions.

Applications of blockchain-based tokens in the energy sector

In our analysis of related work, we found general agreement that digital solutions are required for the recording, exchange, and accumulation of fine-granular CO_2 emission information that is essential for products with a complex production and usage life cycle (Al Sadawi et al. 2021). In this context, publications like (Pigeolet and Van Waeyenberge 2019; Jackson et al. 2018) emphasize the importance of establishing interoperability and trust in the correct documentation of CO_2 emissions not only across businesses but also across domains and legislations. As these two objectives can be difficult to achieve in siloed IS, researchers—also from the Energy Informatics community—have repeatedly proposed blockchain technology as a technical basis for CO_2 emission documentation or trading (Al Sadawi et al. 2021; Albrecht et al. 2018; Richard et al. 2019; Jackson et al. 2018). Blockchain undoubtedly brings several characteristics that seem appealing in this context, for instance, it offers a neutral platform that even mutually distrusting stakeholders can agree on Fridgen et al. (2018), and it facilitates the exchange of value by avoiding the double spending of digital assets. These assets can either be defined purely inside a blockchain or represent existing physical or digital objects. Several projects, like Toucan, RegenNetwork, Moss, or KlimaDAO, focus on the hitherto less transparent market for voluntary CO_2 offsetting. These markets offer the opportunity to invest in projects that aim to consume CO_2. In order to provide the often missing transparency and to prevent the "double spending" of CO_2 offsets, they rely on a blockchain-based infrastructure. However, such projects do not consider the necessary identification of emissions that would enable a CO_2-adaptive decision making as we discuss in this paper but rather their compensation.

Blockchain technology achieves decentralized platforms by replicated information processing and consensus on what is the correct state of the ledger (Butijn et al. 2020). It, thus, carries a high degree of transparency and can enforce implemented rules.

However, transparency in this context is a two-sided sword: Information on a businesses' CO_2 emissions can be problematic because it constitutes sensitive business data that may allow competitors to infer information that they should not get access to or even conflict with antitrust regulation (Sedlmeir et al. 2022; Schellinger et al. 2022). In a downstream approach, CO_2 emission data could even become personally identifiable and, thus, conflict with data protection regulation and end users' privacy requirements. As blockchains only provide pseudonymization and their transparency typically enable linking transactions, their use is, thus, problematic, and additional privacy-enhancing technologies must be applied (Körner et al. 2022; Munilla Garrido et al. 2021; Sedlmeir et al. 2022). There are also "traditional" types of ledgers which can be more or fully centralized and also can have different models for accessing data and publishing new data to the ledger. These can reduce privacy issues, since they only grant access to the data to a predefined group, but especially for sensitive data like energy usage this can still be problematic. A very popular approach to solve privacy issues in blockchain-based systems (and that could also be used in centralized systems) are so-called shielded transactions, for example, in Zcash or Monero, which hide both identities and exchanged values. However, unlike cryptocurrencies, where the total supply is either an invariant or follows strictly defined rules, CO_2 emission systems are not closed: CO_2 emissions data needs to be fed into the system permanently and reliably. In the context of blockchain, this is often referred to as the "oracle problem". Consequently, some degree of transparency with respect to amounts and identities that are responsible for the emission needs to be present, and emissions have to be distinguishable with respect to their source and history to reflect this property. Such "distinguishable" objects are commonly represented by NFTs on blockchains.

There are also NFTs that allow the ownership of parts of the asset represented by them. This is called *fractional ownership* (cf. Implementation section). Such a splitting of distinguishable objects between multiple entities has already been suggested, for instance, in the context of art markets and creative work (Barbereau et al. 2022; Whitaker and Kräussl 2020) and real estate (Sunyaev et al. 2021; Bechtel et al. 2022). We aim to apply fractional ownership to facilitate the splitting and aggregation of CO_2 emission information in the electricity system's supply chain.

Privacy-preserving (non-)fungible tokens in other research areas

It is precisely the design of a CO_2 emission tracing system that satisfies verifiability, distinguishability, fractional ownership, and privacy that we want to contribute to. Common NFTs, like implemented in the ERC-721 token standard on the Ethereum blockchain (Ethereum Foundation 2022), offer transparency and distinguishability as well as fractional ownership, but fail to provide privacy. On the other hand, privacy-oriented payment solutions like ZCash offer privacy and transparency corresponding to the currency's set of rules, but do not offer distinguishability. A combination of privacy and non-fungibility is often referred to as shielded NFTs, as implemented for instance in EY's Nightfall (EYBlockchain 2020). This approach to shielded NFTs comes closest to what we aim for, but so far, to the best of our knowledge, there are no shielded NFTs that allow for fractional ownership. In this sense, our approach is not only the first to combine the necessary requirements, i.e., verifiability, distinguishability, fractional

ownership, and privacy, for CO_2 tracing systems but also closes the technical gap of implementing shielded NFTs with fractional ownership.

Implementation

Technical background

In order to discuss and compare different existing approaches with the one we present in the following, we provide a common understanding about relevant cryptographic basics. We start with hash functions, which are an essential component of most cryptographic systems (Schneier 2017). A hash function H is a deterministic function that maps an input x of arbitrary length to an output y of fixed, relatively short, length, aiming to fulfill two essential properties. First, hash functions should be one-way functions, meaning that it is very difficult—nearly impossible—to determine the input x given an output $y = H(x)$, we call this pre-image resistance. Second, they should be collision resistant, which means that it is very difficult to find two inputs x_1 and x_2 sharing the same output y, i.e., $H(x_1) = H(x_2)$ cannot be solved efficiently when $x_1 \neq x_2$.

Another essential building block of most blockchain systems are Merkle trees (Merkle 1988). They combine the hierarchical data structure of a tree with the utility of hash functions with the purpose of representing multiple data points efficiently under a single hash. A tree, in general, is a data structure consisting of multiple data points called nodes. Starting from the first node, called the root, every (parent) node has child nodes, which themselves have child nodes, and so on, until the lowest level of nodes is reached. We call these nodes without own child leaves. Each leaf of a Merkle tree represents a hash of one of the data points. Each parent node consists of the hash of the concatenation of all its child nodes. Thereby, each parent node represents its child nodes, and the Merkle root represents all data points (leaves) of the tree. When we speak about Merkle trees, we mean by default fully perfect binary trees, this type of tree consists of nodes having either two or no child nodes and leaves having the same number of (in)direct parent nodes. Besides the properties of hash functions such as pre-image and collision resistance, Merkle trees provide so-called Merkle proofs, which offer the possibility to prove that a data point is part of the tree, represented by the Merkle root, without having to include other data points directly in this proof. In order to do so, the prover just requires the "path" of the data point inside the tree, which are all nodes of the tree with which the leaf of the data point is directly or indirectly hashed. Thereby, pre-image resistance prevents from reconstructing any other data point and collision resistance from creating Merkle proofs for data points which are not part of the tree. The required storage for Merkle trees grows constantly with the number of data points it represents, but the size of a Merkle proof only grows logarithmically.

The third cryptographic building block we use are Zero-Knowledge Proofs (ZKPs). The fundamental concept of a ZKP is to generate a proof that a statement is true, without revealing more useful information than the statement itself (Goldwasser et al. 1989). Examples are proving that a computation for a known output was done correctly without redoing the whole computation process or verifiably showing that one has a certain piece of information that leads to a given hash without presenting it. Like most other cryptographic concepts, ZKPs are based on the hardness of cryptographic problems, meaning that it is "practically infeasable" to generate a valid proof from a false statement. One of

the most popular zero-knowledge proving systems for relatively general computer programs are Succinct Non-interactive Arguments of Knowledge (SNARKs) (Ben-Sasson et al. 2013). They consist of two main steps: First, representing a computer program by a polynomial, which is possible for all finite programs, and second proving that the polynomial has specific roots, which could only be obtained if the program was executed correctly, without revealing the full polynomial. For the conversion, so called "circuits" are defined, which represent a computer program as a closed system. Each circuit has a fixed number of constraints that corresponds to the degree of the polynomial required for the proof and depends on the complexity of the underlying computer program. In practice, these circuits need to be optimized to have acceptable computational costs. Specifically, hash functions like SHA256 (Appel 2015) involve many constraints, which is why hash functions specialized for ZKPs, such as Poseidon (Grassi et al. 2021), often find application. The second step, proving the knowledge of a polynomial with specific roots, is based on basic polynomial properties, especially the factorization of polynomials and the fact that two non-identical polynomials of degree d cannot have more than d points of intersection. For SNARKs, this is combined with other cryptographic primitives such as partially homomorphic encryption and pairings of elliptic curves. On the other hand, there are also ZKPs that only require secure hash functions for their construction, called Scalable Transparent Arguments of Knowledge (STARKs) (Ben-Sasson et al. 2019).

Implementation of privacy-preserving NFTs in detail

After giving an overview of different approaches and preliminary work, we will use the following section to present our implementation of privacy-preserving, fractionalizable NFTs. We start by introducing related, existing implementations that fulfill some of the requirements of our system. Subsequently, we explain our implementation in detail. As discussed earlier, an implementation of a documentation and trading system for carbon emissions needs to satisfy at least the following requirements: Verifiability, distinguishability (non-fungibility), traceability, support of fractional ownership, and privacy, including GDPR-compliance. As, for example, the Bitcoin blockchain satisfies verifiability of transactions and NFT standards on Ethereum smart contracts moreover provide distinguishable and traceable digital assets, fractionality and privacy have not yet become a widely known practice. To the best of our knowledge, there are no current implementations for privacy-preserving (shielded) NFTs with fractional ownership, especially not in the application of emission tracing. As we build on and extend existing approaches, we want to present and discuss them briefly.

The implementation of NFTs facilitates non-fungibility in blockchain-based systems. The ERC-721 token standard is the first standardized implementation of NFTs on the Ethereum blockchain. The subsequent ERC-1155 standard combines fungible (ERC-20) and non-fungible (ERC-721) tokens and additionally enables splitting them for fractional ownership. On the other hand, these standards do not provides strong privacy guarantees because—while user addresses are pseudonymous—transactions are linkable (Biryukov et al. 2014; Pfitzmann and Hansen 2010). Zcash on the other hand, which was proposed by Sasson et al. (2014) and is one of the first blockchain-based solutions for anonymous "electronic cash", offers different privacy and transparency options, depending on the type of transaction, but does not provide distinguishability. It uses Merkle

trees to store the different transactions and ZKPs to verify them without revealing information to the public. Yet, Zcash is limited to simple payments with fungible tokens. The cryptocurrency Tezos with its Sapling integration (Nomadic Labs 2021) adopts the concept (and partially even the implementation) of Zcash but applies it inside smart contracts. Thereby, it enables private transactions for other tokens than just the blockchain native token, but the privacy is still limited to fungible tokens. EYs nightfall implementation (EYBlockchain 2020), which is usable on Ethereum and other EVM-compatible blockchains, further develops Tezos' sapling implementation and adds the possibility to transact non-fungible tokens. With this, Nightfall provides private transactions for NFTs, making it the implementation that fulfills the most of our requirements, but still misses the fractionalizability of the shielded NFTs.

For our prototype, we took the Zcash approach introduced in Sasson et al. (2014) as a basis. This approach builds on top of the Unspent Transaction Outputs (UTXO) model, first introduced by Bitcoin, and combines it with ZKPs constructed with SNARKs to achieve full privacy in its native token transfers. A transfer involves consuming some of the sender's UTXOs and creating new UTXOs. The sender issues a new UTXOs, which comprises a public key and an amount, to the receiver address. Since UTXOs can only be spent in their entirety, in most cases the sender issues a second UTXO to its own address again. Its value results of the old coins minus the value of the new coins, i.e., this UTXO in some sense represents the change of the transaction. Everyone can verify that a UTXO has not been spent before and that the total input and output values match. As the sender can issue every new UTXO to a new public key (address), it seems privacy-oriented at first. However, the direct linkage of spent and newly created UTXOs in fact allows to de-anonymize most transactions using more sophisticated tools (Biryukov et al. 2014). Consequently, to enhance privacy and to hide sensitive information on the public blockchain ledger, Zcash does not verify transactions based on a publicly linkable transaction history. Using hash functions and adding some randomness as entropy ("salt"), one can easily hide all transaction details, including transaction addresses, spent coins, received coins, and change, which are usually visible to all network participants. We call these salted hashes of the context of each UTXO commitment. A private ("shielded") Zcash transaction hence has to involve a proof of knowledge of all pre-images of a all involved commitments to ensure that the transaction actually corresponds to a commitment in history and that all new commitments are valid. This involves, for example, to prove the ownership of a commitment and to ensure constant supply, i.e., to prevent the creation of new tokens from thin air. To make sure that one cannot spend coins multiple times, the commitment needs to be "nullified", i.e., tagged as "spent". However, to ensure the unlinkability required for anonymous transactions, there must be no direct pointer to the UTXOs consumed and created in a transfer. Hence, a Merkle tree of initially fixed (large) size bundles all commitments, where each leaf represents one commitment. When conducting a new transaction that creates two new commitments, the blockchain nodes add the commitments to the Merkle tree and post the Merkle root of that new resulting tree on the blockchain. This makes it possible for the owner of a commitment to verify its existence by a proof of membership in the Merkle tree. This proof of membership validates a Merkle proof for a certain commitment through a ZKP and publishes only the corresponding Merkle root, which has to exist on the ledger at

any point of time. Additionally, the sender creates a nullifier for the commitment, which will also be appended to the blockchain. Knowing the pre-image of all involved UTXOs' commitments, the sender's ZKP also proves—without revealing the commitment or the associated transfer amount and addresses involved—that: (1) the new commitments create no new coins, i.e., the total amount in the spent UTXOs equals the total amount in the newly created UTXOs, (2) the spending commitment exists (proof of membership), (3) the sender owns the spending commitments, i.e., knows the associated private key, (4) the sender correctly derives the nullifier from the pre-image of the spending commitment. To process a transfer, consisting of a ZKP, two commitments, a nullifer, and a Merkle root, the network checks the statements (1)–(4) and that the revealed nullifier has not been published before. If all this is true, the network adds the commitments to the tree (and updates the Merkle root accordingly) and appends the nullifer to the corresponding list.

To account for the intended distinguishability, i.e., non-fungibility of CO_2 certificates represented by shielded UTXOs, we adapt the approach of Zcash and add further information to the commitments' pre-images. Hereby, we essentially make them represent shielded (fractional) NFT transfers. The pre-image of each commitment in our approach contains the following attributes:

- Hash: The hash of the object the NFT represents (e.g., emission certificate).
- Quantity: The share of the object represented by this UTXO.
- Public Key: The NFT owner's public key.
- Consumed: Marks the NFT as consumed when the represented object no longer exists.
- Salt: Ensures that each commitment is unique through adding entropy.

The CO_2 emissions tracing implementation we present here can be managed by blockchain technology, just like Zcash. However, as a large-scale and fine-granular carbon market would arguably have higher requirements on throughput in the future and as we do not focus on performance improvements in this paper, we assume instead that a central institution manages the associated ledger, which we call ledger authority. Due to the privacy-by-design of our approach, businesses and end-users must trust this institution only with regard to integrity and non-censorship, but not with their sensitive information.

Although we assume that a central instance can manage the ledger without restricting the privacy of the users, the initial creation of the NFTs ("minting") should rely on a central institution alone, since this again requires access to partially sensitive data and creates several challenges regarding scalability when aiming for a fine-granular tracing system. This is why the verification of CO_2 emission data and the subsequent minting of certificates should be carried out as decentralized as possible. We aim for a system in which each emission-relevant plant is capable of minting its NFTs on its own. For this purpose, we assume that trust-creating parties embed trustworthy sensors in each of these plants. Each sensor has a unique and non-transferable public-private key pair, on behalf of which it is capable of minting new NFTs. In this digital identity approach, the trust-creating parties report all trustworthy public keys to the ledger authority, which

writes them on a safelist holding all public keys authorized for minting. To avoid that every minter has to authenticate with their public key every time they create a NFTs, the safelist is represented by another Merkle tree holding one public key in each leaf. Hereby a minter can utilize a proof of membership on the safelist tree to avoid showing its public key. To ensure private transaction creation, we require that both the commitment and safelist Merkle tree have public read access. However, if the respective use case desires a decentralized management of the ledger, our approach can operate without further concerns regarding the privacy of transactions, etc., within a blockchain infrastructure.

Figure 1 features the ZKP's main statements for a minting transaction. In our nomenclature, INPUTS are private (the prover does not reveal them) yet some of the private inputs may be exchanged between sender (prover) and receiver [for instance, the receiver's Public Key (PK)], OUTPUTS are public (they need to be disclosed for verification of the ZKP). To mint a new NFT, the minter creates and sends a valid minting-ZKP, the Merkle root of the current safelist, and the new commitment to the ledger authority. Subsequently, the authority verifies the ZKP, checks if the safelist's root matches to the one stored on the ledger, and finally adds the commitment to the ledger. This transaction does not disclose the miner's identity or any details about the NFT.

As in Zcash, a nullifier must invalidate a commitment; therefore, there are two properties that it should fulfill. First, it must be bound to the pre-image of the commitment (without being linkable to the value of the commitment) and second, it should only be possible for the owner of the commitment to create it. Therefore, we chose an implementation where the pre-image of the nullifier includes the signature of the commitment itself using the Secret Key (SK) corresponding to the commitments PK: $\text{nullifier} = \text{Hash}(\text{Signature}(\text{SK}, \text{commitment}))$. Previous to the proof generation, the receiver sends its PK to the sender. Due to the fact that the commitment Merkle tree has public access rights, senders can generate a proof of membership for their commitment by their own. Consequently, senders have all information for creating the ZKP, which Fig. 2 describes. Since the nullifier consists of a signature of the commitment and its pre-image contains its owner's PK, only the holder of the matching SK (owner of the NFT) is capable of generating the nullifier and therefore spending the commitment. Thus, the sender submits the Merkle root, the nullifier, and the two new commitments along with the transfer-ZKP, which confirms the correct generation of all these hashes (commitments and nullifier) to the ledger authority. The authority validates the ZKP and checks whether the Merkle root existed at some point in history. If these conditions are met, the ledger authority adds the receiver and change commitment to the tree, updates the new Merkle root, and appends the nullifier to the list. At this point, the ledger authority

Minting
INPUT: Pre-image of new commitment, minter's PK, Merkle proof on the safelist for minters' PK, salt
OUTPUT: Merkle root of safelist, new commitment
CHECKING THAT:
- *The Merkle proof for the safelist is valid*
- *The pre-image of the new commitment is valid*

Fig. 1 Zero-Knowledge Proof—Minting

Transfer
INPUT: Pre-image of sender commitment, amount, PK of the receiver, salts for the change and receiver commitment, nullifier of the sender commitment, Merkle proof for the sender commitment
OUTPUT: Merkle root, nullifier of the sender commitment, receiver commitment, change commitment
CHECKING THAT:
- *The Merkle proof of the sender commitment is valid*
- *The accounting is correct; amount* > 0*; sender = receiver + change*
- *The pre-image of the nullifier is correct, was not published already and corresponds to the commitment*
- *The pre-image of the receiver commitment is correct*
- *The pre-image of the change commitment is correct*

Fig. 2 Zero-Knowledge Proof—Transfer

already settled the transaction by storing it on the ledger, but transaction recipients cannot realize or even utilize this yet. Consequently, the sender has to send the transaction receiver the pre-image of the newly added receiver commitment. Finally, the recipient can verify the pre-image of the transaction by comparing its hash to the commitments on the ledger. As the sender issued the receiver commitment to the receiver's PK the receiver is now capable of proving the ownership or spending the NFT on behalf of its SK.

Application for the case of charging electric vehicles

As mentioned above, we exemplary apply our approach for the use case of charging electric vehicles, where we aim to provide verifiable data to the end-consumer, for example, the owner of an electric vehicle. This data entails information about the CO_2 emissions that are associated with the amount of electricity that has been charged. Of course, this information is aggregated and disaggregated along the accounting or contractual path of the electricity—and not along the physical path, which is not possible to trace.

Figure 3 illustrates the application of shielded fractionalized NFTs for a proof-of-origin of green electricity. To simplify this illustration, we present a self-contained scenario with few stakeholders involved. Any further transfers between additional participants would be integrated in the same way. In our scenario, we consider a windmill that generates electricity. The windmill is owned by an electric utility. This electric utility directly sells electricity to an electric vehicle, which charges its battery at one of the electric utility's charging point. We assume that the windmill generates at least that much electricity the electric vehicles consumes. The electric utility advertises to issue certificates of origin for each delivery, with a temporal granularity of 15 min.

In order to address the oracle problem and ensure the correctness of external data that is fed into the system, we further assume that during the construction of the plant, a trustworthy third party ("certifying party") installed a tamper-proof sensor unit and adds the sensor's public key to the safelist tree on the ledger. The sensor unit signs all measurements of electricity generation and a factor of proportionality for the associated carbon equivalent emissions using asymmetric encryption. In a more complex real-world

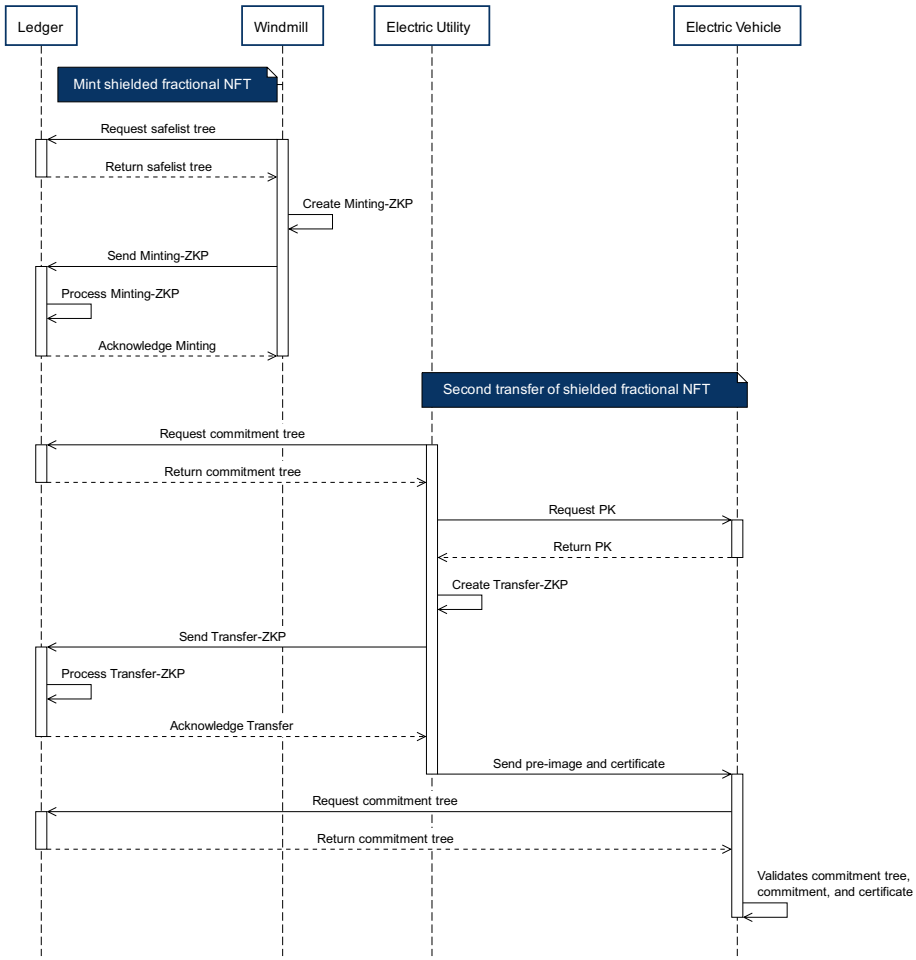

Fig. 3 Process of minting and transfer of proof-of-origin certificates

setting, one would arguably use certificate chains and only add the public keys of some root certificates to the registry. Further, the certifying party issues a digital certificate about the plant's master data in the computing environment of the sensor. Restricting the minting of NFTs only to the sensor's secure environment reduces the risk of fake certificates. Further, if a participant detects an anomaly for an NFT, the information attached to it, i.e., the corresponding asset's master data, enables tracing to the source of it.

We assume that the plant produces 100 kWh in each 15 min interval, with almost zero associated CO_2 emissions, as the windmill is a renewable energy source. Consequently, in each interval, the windmill mints a new proof-of-origin NFT for the amount of electric energy produced. The certificate of origin associated with the NFT—which represents the pre-image of the corresponding commitment—is structured as described above and consists of the following attributes:

- Hash (Certificate): The hash value of the proof-of-origin certificate represented by the NFT. It holds the time interval in which the plant produced the electricity and all relevant master data of the plant. The certificate may look like:

  - Production timestamp: 2022-04-20T07:30:00 + 02:00
  - Plant type: Windmill
  - Plant location: Bavaria, Germany
  - Factor of proportionality for carbon emissions (kg CO_2eq): 0
  - Year of construction: 2007
  - ...

- Quantity (kWh): 100
- Public Key: 0×1234 (Must be included in the safelist)
- Salt: 4853

After collecting all this data, the plant requests the current safelist tree from the ledger. Based on this information, the plant creates the Minting-ZKP, which includes a proof that the PK in the certificate is contained in the safelist tree, and sends it to the ledger authority. The ledger authority validates the ZKP and adds the newly minted commitment to the global commitment tree. As soon as the ledger authority has added the new commitment and notified the windmill in an acknowledgement of successful minting, the windmill transfers the newly minted NFT entirely to the electricity utility. This first transfer process takes place analogous to the next transfer, which we describe in detail.

The electric vehicle charged exactly 10 kWh during the first 15 min interval. The forgery-proof, certified sensors in the vehicle and the charging point trustfully record this consumption. According to this record, the electricity utility forwards a fraction of the NFT—10% of it—to the electric vehicle. To do so, the electricity utility first requests the current commitment tree from the ledger and the vehicle's PK, which represents the receiver address. With this information, the electricity utility can extract a Merkle proof of its possession of the full (share of 100%) of the NFTs. It then consumes this share and creates two new fractionalized NFT from it, which add up to 100%. The electric vehicle's NFT includes the following information:

- Hash (Certificate): Exactly the same hash representing the same proof-of-origin certificate as minted previously by the windmill
- Quantity (kWh): 10
- Public Key: 0×2345 (PK of the electric vehicle)
- Salt: 9132

The other NFT contains the "change", i.e., the rest of the fractionalized NFT which stays at the utility:

- Hash (Certificate): Exactly the same hash representing the same proof-of-origin certificate as minted previously by the windmill
- Quantity (kWh): 90
- Public Key: 0×1234 (PK of the electric utility)
- Salt: 1252

For this transfer, the electric utility creates a Transfer-ZKP and sends it to the ledger authority. After checking the Transfer-ZKP and whether the nullifier has been published before, the ledger authority updates the ledger and sends a confirmation receipt for the transfer to the electricity utility. Subsequently, the electricity utility informs the electric vehicle about the transfer by sending the pre-image containing inter alia the proof-of-origin certificate of the new NFT. The electric vehicle checks if the NFT is now indeed in its possession by checking the correctness of the pre-image, for instance, the PK. In addition it checks using the current commitment tree if the new NFT is also settled on the ledger.

This process will be repeated for all time intervals in which the vehicle is charging. For example, if the vehicle charges for one hour, it will receive four of these proof of origin certificates represented by fractionalized NFTs in the end and can clearly trace to which plant the consumed electricity is attributable. They can also compute the CO_2 emissions associated with their proof of origin by multiplying the original certificate's factor of proportionality for carbon emissions (kg CO2eq) with the amount of electricity represented by the NFT that they own, i.e, its "quantity". Thus, our approach enables end-consumers to trace and cryptographically verify emission data by using anonymized data on the ledger.

Contribution and discussion

This section briefly highlights the contributions to research and practice resulting from our work. In addition, it discusses corresponding implications of our research.

Overall, our paper outlines a new concept for CO_2 emission tracing in the course of the energy transition that enables an end-to-end connection, i.e., data exchange, between energy supplying and energy demanding assets by shielded NFTs with fractional ownership. Our approach boils down to the bilateral, digital exchange of distinguishable and divisible carbon certificates with a blockchain-based, fully anonymous double spending prevention. Moreover, this paper also demonstrates our concept's applicability by a prototypical implementation.

Our concept provides end consumers with real-time information about the consumed CO_2 emissions associated with the amount of electricity bought. Here, the "amount of electricity bought" refers to the business-sided, i.e, contractual, transactions of electricity while the physical delivery of electricity, i.e., electrons, is not traceable in modern electricity systems, of course. Against this background, our concept enables an end-to-end verifiable traceability of fine-granluar CO_2 emissions in energy systems in (close to) real-time. Since such a concept for fine-granular tracing of emission data produces sensitive data, it is mandatory to consider the protection of this data at an early stage. Most approaches are based on the concept of privacy-by-trust, which relies on the assumption that certain parties handle sensitive data in a trustworthy manner. We based the approach presented in this paper strictly to the idea of privacy-by-design, according to which no sensitive data become accessible to third parties. Hence, our research is the necessary foundation for a CO_2 adaptive decision making, for example, in energy-intensive industries. Moreover, it may be the foundation for future carbon trading markets.

Regarding our concept's applicability, which is highly needed in the course of energy informatics (cf., among others, Staudt et al. 2019), we find that already with a prototypical implementation on commodity hardware and a centralized ledger, our approach has practical performance, specifically on the end user side. Using the Poseidon hash function, our circuit has around 10, 000 Rank 1 Constraint System (R1CS) constraints. We tested performance on an Ubuntu 20.04 virtual machine with 4 virtual cores and 16 GB or RAM allocated, running on a commercial standard laptop (Dell Latitude 7400 with an Intel i7 8665U CPU). We averaged our time measurements over 100 iterations for each operation. Proof creation—the most computationally intensive operation in the Groth16 SNARK system (Groth 2016)—takes around 4.0 s when using the default setting that used Web assembly for witness generation and JavaScript for proof generation. The (static) proving key that needs to be stored for creating proofs has a size of around 6.3 MB, the (static) verification key needed for verification of around 3.5 kB. The size of the proof itself is less than 1 kB. These figures suggest that proof creation could be practical on a mobile phone, too. With a more optimized tool for proof generation, performance can even be improved considerably: With witness generation in C++ and the "Rapidsnark" software (Hermez Network 2021) that uses ×86 Assembly, the time for proof generation is only 0.23 s. So far, there is no optimized software for proof verification, which correspondingly takes around 1.0 s in JavaScript. Other libraries claim to have verification times of less than 10 ms for similar Groth16 SNARKs (Amine et al. 2020). In summary, we conclude that our approach is implementable in practice.

This paper contributes to the body of knowledge of both, of the computer science and applied cryptography community by demonstrating an implementation for shielded NFTs with fractional ownership, and of the energy informatics community by developing a new concept for applicable and target-oriented CO_2 emission tracing. Moreover, our research holds various contributions for practice as it may impact both, businesses and policy. Regarding the latter, policy may challenge existing approaches, e.g., the EU-ETS, that aim at decreasing CO_2 tracking emissions while not being able to provide high temporal and quantitative granularity of CO_2 emissions. Against this background, policy-makers must reconsider the targets they would aim for and they must evaluate how to develop existing approaches further. Regarding businesses, our concept enables various potential benefits that range from the possibility to provide product-specific CO_2 emission information to end consumers, e.g., in the case of e-mobility charging, to the enabling of CO_2-adaptive decision making or process management, e.g., in the case of industrial manufacturing. Thinking further, our concept may also be the technical cornerstone for any information to be reported in complex and international supply networks, for example, in the context of future regulation on keeping conditions of the sustainable development goals.

Conclusion

In this paper, we outline a technically and substantively new approach for CO_2 emission tracing in energy systems by using shielded NFTs with fractional ownership to enable an end-to-end verifiability of emission data. Our approach integrates both businesses and

end consumers on a transparent, decentralized architecture while addressing privacy-relevant requirements. Against the background that primary and verifiable CO_2 data is not available to end consumers, so far, and for enterprises merely in scope of a one year period, we consider our approach an enabler of a CO_2-adaptive decision making for end consumers and businesses that is one of the keys for promoting the energy transition (Strüker et al. 2021). Our concept builds on established cryptographic primitives like hash functions, Merkle trees, and digital signatures, in combination with blockchain-based NFTs and ZKPs. Building on previous privacy-oriented constructions of blockchain-based tokens such as Sasson et al. (2014) or Nightfall (EYBlockchain 2020), we implement fractional ownership for shielded NFTs, which are linked to digital certificates stored and exchanged off-chain that include detailed information on carbon emissions and, thus, prevent double usage of CO_2 certificates through a transparent public ledger without disclosing additional information (privacy-by-design). Our approach hence allows us to leverage the benefits of a decentralized architecture in terms of openness and transparency as pointed out by related work, yet keeps information on stakeholders' CO_2 emission data completely confidential without compromising traceability. We illustrate the applicability of our concept by a prototypical implementation and discuss corresponding contributions and implications, e.g., its benefits for information availability, traceability, and verifiability and the associated opportunities on deep decarbonization. Our approach may also be promising in more general settings, for instance, for the exchange and verification of dynamic data and specifically quantitative proofs of origin in complex supply networks—a challenge that several publications have pointed to (Sedlmeir et al. 2022; Platt et al. 2021).

Nevertheless, our research is subject to several limitations. First of all, we have not benchmarked the system in long-term and large scale use cases yet. Moreover, the concept that we develop in this paper as well as its applicability is only described in the narrow context of tracing CO_2 emissions when charging an electric vehicle. That means it does not yet include functionalities for CO_2 trading or a corresponding market, as our approach currently focuses on establishing a positive registry that cannot enforce stakeholders to pay for holding CO_2 certificates (fractions of shielded NFTs). We aim to connect this registry with existing frameworks which, for instance, incorporate such a billing process at the end of a specific epoch. This could be achieved, for instance, through governance processes that require an exchange of CO_2 certificates in every business interaction, or through cryptographic approaches like anonymized, account-based systems linked to stakeholders' digital identities, as described in Gross et al. (2021).

We believe that our approach could be a promising and inspiring starting point for further research. Scholars may evaluate how to develop our approach so that it can establish a CO_2 trading market. Moreover, future research may consider the role of CO_2 budgets for citizens, i.e., end consumers, against this background. From a practical perspective, we close the gap between existing concepts for CO_2 tracing and their confidentiality and traceability requirements and present an open approach that may help avoid fragmented systems with boundaries. Regarding a comprehensive implementation of such a system, policy-oriented scholars may elaborate on how to bring this system to practice. Furthermore, real world implementations have to further address the oracle problem to ensure the integrity of external data that decentralized sources feed into

the system. Research regarding this problem can be both on a high, application overarching level, as well as focused on solving the oracle problem for specific applications of the system. Although researcher and practitioners already discuss this problem and develop general solutions, an application specific transfer of this research stream is still needed. From a technical perspective, our approach's performance in a large-scale system could be considered in more detail and the suitability of improvements, for instance, incremental optimizations of performance through optimizing cryptographic primitives involved in the ZKP circuits, general scalability solutions for blockchains such as sharding and rollups, or other compression techniques for ZKPs like Gailly et al. (2021) or recursion, which is not yet available with the implementation of the Groth16 proof system that we used but with alternative systems like Plonky2 (Farmer 2022). In sum, the research question how to design an interoperable, scalable IS for tracing CO_2 emissions remains a highly relevant and exciting interdisciplinary endeavour that requires research on the intersection between economic (energy markets) and technical (applied cryptography, high-performance systems) scholars.

Acknowledgements
We thank Felix Paetzold for his valuable feedback on the manuscript.

About this supplement
This article has been published as part of Energy Informatics Volume 5 Supplement 1, 2022: Proceedings of the 11th DACH+ Conference on Energy Informatics. The full contents of the supplement are available online at https://energyinformatics.springeropen.com/articles/supplements/volume-5-supplement-1.

Author contributions
MB: Project administration, Conceptualization, Implementation, Writing—Original Draft. VG: Implementation, Writing—Original Draft. M-FK: Conceptualization, Writing—Original Draft. JS: Conceptualization, Validation, Writing—Original Draft. JS: Supervision, Writing—Review and Editing. TZ: Writing—Original Draft. All authors read and approved the final manuscript.

Funding
We gratefully acknowledge the financial support of the project "ID-Ideal" (Grant-Number: 01MN21001I) by the Federal Ministry for Economic Affairs and Climate Action (BMWK) and the project supervision by the project management organization DLR.

Availability of data and materials
There is no additional data and materials.

Declarations

Competing interests
The authors declare that they have no competing interests.

Published: 7 September 2022

References

Ahi P, Searcy C (2015) An analysis of metrics used to measure performance in green and sustainable supply chains. J Clean Prod 86:360–377

Al Sadawi A, Madani B, Saboor S, Ndiaye M, Abu-Lebdeh G (2021) A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract. Technol Forecast Soc Chang 173:121124

Albrecht S, Reichert S, Schmid J, Strüker J, Neumann D, Fridgen G (2018) Dynamics of blockchain implementation—a case study from the energy sector. In: Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 3527–3536

Amine O, Baghery K, Pindado Z, Ràfols C (2020) Simulation Extractable Versions of Groth's zk-SNARK Revisited (2020). https://eprint.iacr.org/2020/1306.pdf Accessed 2022-04-22

Appel AW (2015) Verification of a cryptographic primitive: SHA-256. ACM Trans Program Lang Syst 37(2)

Association of Issuing Bodies: EECS Rules Release 7 v15 (2021). https://www.aib-net.org/eecs/eecsr-rules Accessed 2022-04-22

Barbereau TJ, Smethurst R, Sedlmeir J, Fridgen G, Rieger A (2022) Tokenization and regulatory compliance for art and collectible markets: From regulators' demands for transparency to investors' demands for privacy. In: Lacity M, Treiblmaier H (ed) Blockchains and the token economy: studies in theory and practice. Palgrave Macmillan, Vienna
Baza M, Sherif A, Mahmoud MM, Bakiras S, Alasmary W, Abdallah M, Lin X (2021) Privacy-preserving blockchain-based energy trading schemes for electric vehicles. IEEE Trans Veh Technol 70(9):9369–9384
Bechtel A, Ferreira A, Gross J, Sandner P (2022) The future of payments in a DLT-based European economy: a roadmap. In: The Future of Financial Systems in the Digital Age, pp. 89–116. Springer, Singapore
Beck R, Müller-Bloch C, King JL (2018) Governance in the blockchain economy: a framework and research agenda. J Assoc Inf Syst 1020–1034
Ben-Sasson E, Chiesa A, Genkin D, Tromer E, Virza M (2013) SNARKs for C: Verifying program executions succinctly and in zero knowledge. In: Annual Cryptology Conference, pp. 90–108. Springer, Santa Barbara, USA
Ben-Sasson E, Bentov I, Horesh Y, Riabzev M (2019) Scalable zero knowledge with no trusted setup. In: Annual International Cryptology Conference, pp. 701–732. Springer, Santa Barbara, USA
Biryukov A, Khovratovich D, Pustogarov I (2014) Deanonymisation of clients in Bitcoin P2P network. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 15–29
Björklund M, Martinsen U, Abrahamsson M (2012) Performance measurements in the greening of supply chains. Supply Chain Manag Int J 17(1):29–39
Butijn B-J, Tamburri DA, Heuvel W-Jvd (2020) Blockchains: a systematic multivocal literature review. ACM Comput Surveys 53(3)
Cachin C, Vukolić M (2022) Blockchain consensus protocols in the wild (2017). arXiv:1707.01873 Accessed 2022-04-22
Castellanos JAF, Coll-Mayor D, Notholt JA (2017) Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum blockchain. In: International Conference on Smart Energy Grid Engineering, pp. 367–372. IEEE, Oshawa, Canada
de Lima TD, Franco JF, Lezama F, Soares J, Vale Z (2021) Joint optimal allocation of electric vehicle charging stations and renewable energy sources including CO_2 emissions. Energy Inf 4(2)
Djamali A, Dossow P, Hinterstocker M, Schellinger B, Sedlmeir J, Völter F, Willburger L (2021) Asset logging in the energy sector: a scalable blockchain-based data platform. Energy Inf 4(3)
Ethereum Foundation: ERC-721 Non-Fungible Token Standard (2022). https://ethereum.org/en/developers/docs/standards/tokens/erc-721/ Accessed 2020-04-22
European Commission: Monitoring, reporting and verification of EU ETS emissions (2021). https://ec.europa.eu/clima/eu-action/eu-emissions-trading-system-eu-ets/monitoring-reporting-and-verification-eu-ets-emissions_en Accessed 2022-04-22
EYBlockchain: Nightfall Github repository (2020). https://github.com/EYBlockchain/nightfall Accessed 2022-04-22
Farmer B (2022) Introducing Plonky2. https://blog.polygon.technology/introducing-plonky2/ Accessed 2022-04-22
Financial Times: Heavyweight Investors Demand More Disclosure of Environmental Risks (2021). https://www.ft.com/content/7d23ef7f-33ba-4466-b2f1-2a5dfeba1e33 Accessed 2022-04-22
Fiorini L, Aiello M (2018) Household CO_2-efficient energy management. Energy Inf 1(1):21–34
Fridgen G, Radszuwill S, Urbach N, Utz L (2018) Cross-organizational workflow management using blockchain technology—towards applicability, auditability and automation. In: Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 3507–3517
Fridgen G, Körner M-F, Walters S, Weibelzahl M (2021) Not all doom and gloom: how energy-intensive and temporally flexible data center applications may actually promote renewable energy sources. Bus Inf Syst Eng 63(3):243–256
Fridgen G, Halbrügge S, Körner M-F, Michaelis A, Weibelzahl M (2022) Artificial intelligence in energy demand response: a taxonomy of input data requirements. In: Wirtschaftsinformatik 2022 Proceedings
Fuso Nerini F, Fawcett T, Parag Y, Ekins P (2021) Personal carbon allowances revisited. Nat Sustain 4(12):1025–1031
Gailly N, Maller M, Nitulescu A (2021) SnarkPack: Practical SNARK Aggregation. https://eprint.iacr.org/2021/529 Accessed 2022-04-22
Goebel C, Jacobsen H-A, Del Razo V, Doblander C, Rivera J, Ilg J, Flath C, Schmeck H, Weinhardt C, Pathmaperuma D et al (2014) Energy informatics. Bus Inf Syst Eng 6(1):25–31
Goebel P, Reuter C, Pibernik R, Sichtmann C, Bals L (2018) Purchasing managers' willingness to pay for attributes that constitute sustainability. J Oper Manag 62:44–58
Gola C, Sedlmeir J (2022) Addressing the sustainability of distributed ledger technology. Bank of Italy Occasional Paper (670)
Goldwasser S, Micali S, Rackoff C (1989) The knowledge complexity of interactive proof systems. SIAM J Comput 18(1):186–208
Grassi L, Khovratovich D, Rechberger C, Roy A, Schofnegger M (2021) Poseidon: A new hash function for zero-knowledge proof systems. In: 30th USENIX Security Symposium, pp. 519–535. USENIX Association, virtual event
Groth J (2016) On the size of pairing-based non-interactive arguments. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 305–326. Springer
Gross J, Sedlmeir J, Babel M, Bechtel A, Schellinger B (2021) Designing a Central Bank Digital Currency with Support for Cash-like Privacy. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891121 Accessed 2022-04-22
Hanny L, Körner M-F, Leinauer C, Michaelis A, Strüker J, Weibelzahl M, Weissflog J (2022) How to trade electricity flexibility using artificial intelligence: an integrated algorithmic framework. Proceedings of the 55th Hawaii International Conference on System Sciences, 3589–3598
Hassini E, Surti C, Searcy C (2012) A literature review and a case study of sustainable supply chains with a focus on metrics. Int J Prod Econ 140(1):69–82
Heffron RJ (2021) Energy multinationals challenged by the growth of human rights. Nat Energy 6:849–851
Herbes C, Ramme I (2014) Online marketing of green electricity in Germany—a content analysis of providers' websites. Energy Policy 66:257–266
Hermez Network: Open Sourcing an Ultra-fast zk Prover: Rapidsnark (2021). https://blog.hermez.io/open-sourcing-ultra-fast-zk-prover-rapidsnark/ Accessed 2022-04-22

Hervani AA, Helms MM, Sarkis J (2005) Performance measurement for green supply chain management. An International Journal, Benchmarking
Holly S, Nieße A, Tröschel M, Hammer L, Franzius C, Dmitriyev V, Dorfner J, Veith EM, Harnischmacher C, Greve M, et al (2020) Flexibility management and provision of balancing services with battery-electric automated guided vehicles in the hamburg container terminal altenwerder. Energy Inf 3(1)
IPCC: Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press (2021). https://www.ipcc.ch/report/ar6/wg1/downloads/report/IPCC_AR6_WGI_Full_Report.pdf Accessed 2022-04-22
Jackson A, Lloyd A, Macinante J, Hüwener M (2018) Networked carbon markets: Permissionless innovation with distributed ledgers? In: Transforming Climate Finance and Green Investment with Blockchains, pp. 255–268. Elsevier, Oxford, UK
Klingert S (2018) Mapping data centre business types with power management strategies to identify demand response candidates, pp. 492–498
Knirsch F, Brunner C, Unterweger A, Engel D (2020) Decentralized and permission-less green energy certificates with GECKO. Energy Inf 3(1):1–17
Körner M-F, Sedlmeir J, Weibelzahl M, Fridgen G, Heine M, Neumann C (2022) Systemic risks in electricity systems: a perspective on the potential of digital technologies. Energy Policy 164:112901
Lehtinen J, Ahola T (2010) Is performance measurement suitable for an extended enterprise? Int J Oper Prod Manag 30(2):181–204
Maestrini V, Luzzini D, Maccarrone P, Caniato F (2017) Supply chain performance measurement systems: a systematic review and research agenda. Int J Prod Econ 183:299–315
Märkle-Huß J, Feuerriegel S, Neumann D (2018) Contract durations in the electricity market: causal impact of 15min trading on the EPEX SPOT market. Energy Economics 69:367–378
Merkle RC (1988) A digital signature based on a conventional encryption function. In: CRYPTO '87: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, pp. 369–378. Springer, London
Munilla Garrido G, Sedlmeir J, Uludağ Ö, Alaoui IS, Luckow A, Matthes F (2021) Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: a systematic literature review. J Netw Comput Appl 103465
Nomadic Labs: Sapling integration (2021). https://tezos.gitlab.io/alpha/sapling.html Accessed 2022-04-08
Pfitzmann A, Hansen M (2010) A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management
Pigeolet L, Van Waeyenberge A (2019) Assessment and challenges of carbon markets. Braz J Int Law 16:74
Pina A, Silva C, Ferrão P (2012) The impact of demand side management strategies in the penetration of renewable electricity. Energy 41(1):128–137
Platt M, Bandara RJ, Drăgnoiu A-E, Krishnamoorthy S (2021) Information privacy in decentralized applications. In: Trust Models for Next-Generation Blockchain Ecosystems, pp. 85–104. Springer, Cham
Qorri A, Mujkić Z, Kraslawski A (2018) A conceptual framework for measuring sustainability performance of supply chains. J Clean Prod 189:570–584
Richard P, Mamel S, Vogel L (2019) Blockchain in the Integrated Energy Transition. https://www.dena.de/fileadmin/user_upload/dena-Studie_Blockchain_Integrierte_Energiewende_EN.pdf Accessed 2022-04-22
Rieger A, Roth T, Sedlmeir J, Fridgen G (2022) We need a broader debate on the sustainability of blockchain. Joule
Rouholamini M, Miller CJ, Wang C (2020) Determining consumer's carbon emission obligation through virtual emission tracing in power systems. Environ Prog Sustain Energy 39(1):13279
Sasson EB, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M (2014) Zerocash: Decentralized anonymous payments from Bitcoin. In: IEEE Symposium on Security and Privacy, pp. 459–474
Schellinger B, Völter F, Urbach N, Sedlmeir J (2022) Yes, I do: Marrying blockchain applications with GDPR. In: Proceedings of the 55th Hawaii International Conference on System Sciences, pp. 4631–4640
Schneier B (2017) Applied cryptography: protocols, algorithms and source code in C. Wiley, New York
Sedlmeir J, Buhl HU, Fridgen G, Keller R (2020) The energy consumption of blockchain technology: beyond myth. Bus Inf Syst Eng 62(6):599–608
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 Inf Rev 1(1):20–31
Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N (2022) The transparency challenge of blockchain in organizations. Electronic Markets
Staudt P, Lehnhoff S, Watson R (2019) Energy informatics—call for papers, issue 3/2021. Bus Inf Syst Eng 61(6):767–769
Strüker J, Weibelzahl M, Körner M-F, Kießling A, Franke-Sluijk A, Hermann M (2021) Decarbonisation through digitalisation: proposals for transforming the energy sector. University of Bayreuth, the Project Group Business & Information Systems Engineering of the Fraunhofer FIT and TenneT TSO GmbH. https://epub.uni-bayreuth.de/5762/ Accessed 2022-04-22
Sullivan R, Gouldson A (2012) Does voluntary carbon reporting meet investors' needs? J Clean Prod 36:60–67
Sunyaev A, Kannengießer N, Beck R, Treiblmaier H, Lacity M, Kranz J, Fridgen G, Spankowski U, Luckow A (2021) Token economy. Bus Inf Syst Eng 63(4):457–478
United Nations: Paris Agreement (2015). https://unfccc.int/files/meetings/paris_nov_2015/application/pdf/paris_agreement_english_.pdf Accessed 2022-04-22
United Nations Security Council: Climate Change 'Biggest Threat Modern Humans Have Ever Faced', World-Renowned Naturalist Tells Security Council, Calls for Greater Global Cooperation (2021). https://www.un.org/press/en/2021/sc14445.doc.htmf Accessed 2022-04-22
vom Brocke J, Watson RT, Dwyer C, Elliot S, Melville N (2013) Green information systems: directives for the IS discipline. Commun Assoc Inf Syst 33(1):30
Watanabe R, Robinson G (2005) The European Union emissions trading scheme (EU ETS). Climate Policy 5(1):10–14. https://doi.org/10.1080/14693062.2005.9685537

Watson RT, Boudreau M-C, Chen AJ (2010) Information systems and environmentally sustainable development: energy informatics and new directions for the IS community. MIS Quarterly 34(1):23–38
Whitaker A, Kräussl R (2020) Fractional equity, blockchain, and the future of creative work. Manage Sci 66(10):4594–4611
World Economic Forum: how digital tracing can reduce industrial carbon emissions (2021). https://www.weforum.org/agenda/2021/12/digital-tracing-industrial-carbon-emissions-decarbonization/ Accessed 2022-02-14
Zampou E, Mourtos I, Pramatari K, Seidel S (2022) A design theory for energy and carbon management systems in the supply chain. J Assoc Inf Syst 23(1):329–371
Zhang R, Xue R, Liu L (2019) Security and privacy on blockchain. ACM Comput Surveys 52(3)
Zhou S, Brown MA (2017) Smart meter deployment in Europe: a comparative case study on the impacts of national policy schemes. J Clean Prod 144:22–32

Publisher's Note