IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 4, 2019, accepted March 24, 2019, date of publication April 10, 2019, date of current version April 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909170

DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management

FEDERICO MATTEO BENČIĆ, (Member, IEEE), PAVLE SKOČIR, (Member, IEEE), AND IVANA PODNAR ŽARKO, (Member, IEEE)
Internet of Things Laboratory, Faculty of Electrical Engineering and Computing, University of Zagreb, 10000 Zagreb, Croatia

Corresponding author: Federico Matteo Benčić (federico-matteo.bencic@fer.hr)

This work was supported by the TagItSmart Project through the European Union's Horizon 2020 Research and Innovation Programme under Grant 688061.

ABSTRACT Supply chain management enhanced by the Internet of Things (IoT) solutions integrate special tags (e.g., RFID, NFC, and QR-codes) with products to create Smart Tags, in addition to storing supplemental information about a product, which is also used to track products during their lifecycle. However, a product consumer has to implicitly trust the Smart Tag creator and other stakeholders within the supply chain that they are providing authentic data within a product's tag. The DL-Tags solution steps into this environment to offer a decentralized, privacy-preserving, and verifiable management of Smart Tags during a product's lifecycle. The solution is based on distributed ledger technology (DLT) and uses the Ethereum blockchain to mediate interactions between the stakeholders during a product's exchange process. By reaching a consensus on the product's description and state logged on the blockchain, all involved stakeholders and product consumers can verify the product's authenticity without revealing their identity. The paper describes the DL-Tags solution and includes a cost analysis of all implemented transactions on the Ethereum blockchain. The proposed solution provides evidence of the product's origin and its journey across the supply chain while preventing tag duplication and manipulation. It is among the first documented practical solutions using DLT and IoT for supply chain management, which is designed to be distributed ledger agnostic.

INDEX TERMS Blockchain, distributed ledger technology, supply chain management.

I. INTRODUCTION

Supply chain management relates to complex business-to-business and business-to-customer networks, and is traditionally used to operate and maintain producer's relationships with suppliers, logistics, and customers with a goal to deliver superior customer value at reduced cost [1]. Internet of Things (IoT), as a concept which enables the usage of high volumes of smart devices and actuators connected to the Internet, offers innovative solutions for tracking the flow of products and materials relevant to supply chains. In particular, it addresses the main requirement of supply chain management—seamless sharing of product-related information between stakeholders involved in a product lifecycle. IoT-based solutions enhanced by Distributed Ledger Technology (DLT) go even a step further to facilitate a sustainable, decentralized and privacy-preserving information sharing model without a trusted intermediary. Supply chain management has indeed been identified as one of the main applications combining blockchain technology with IoT [2], since involved stakeholders share/exchange product-related data within a trustless environment, but have the possibility to verify product authenticity and agree on its current state.

The TagItSmart (TIS) system is an IoT-based solution for supply chain management which issues product's Smart Tags and supports sharing of product-related information between stakeholders involved in a product lifecycle using such tags [3]. Smart Tags are typically provided in the form of dynamic QR codes printed with special ink. Dynamic QR codes change due to specific environmental conditions (e.g., temperature, humidity, light intensity), and are adequate for tracking of fast moving consumer goods (FMCG) and their surrounding conditions. A product enhanced with its Smart Tag becomes a *digital product* enabling innovative services

The associate editor coordinating the review of this manuscript and approving it for publication was Giacomo Verticale.

across the entire supply chain, from manufacturer, logistics, and retail, to consumer and recycling. However, by using the TIS infrastructure in a centralized setup, a product consumer has to implicitly trust the TIS platform as the Smart Tag creator, as well as other stakeholders in the supply chain, that they are providing authentic data about a product without tempering with its Smart Tag.

DL-Tags steps into this environment as a solution for verifying shared product information in a privacy-preserving and decentralized way, under the assumption that a single centralized authority should be avoided to orchestrate the relevant processes. Since data authenticity and integrity are vital to ensure sustainable management of supply chains, DL-Tags uses DLT, in particular the *Ethereum blockchain*, as a decentralized intermediary adequate for environments involving many stakeholders which do not trust each other [4], [5]. By using the DL-Tags solution, stakeholders are required to reach consensus about the information stored in Smart Tags that is logged on the blockchain. This prevents the possibility to blame one of the former stakeholders in the product lifecycle for unacceptable facts being stored in a Smart Tag. Furthermore, the proposed solution enables *brand protection*: End consumers can verify whether a product belongs to a certain brand as advertised, and to verify that the changes of product ownership along the supply chain is acknowledged by all stakeholders. For example, the proposed solution can be applied in online shopping use cases where e-commerce stores serve as retailers of physical products. One of the reasons why consumers are reluctant to shop online is because they are concerned whether declared information about a product is indeed genuine or not. The main benefit of DL-Tags for end consumers is in the following: Consumers can simply verify product provenance and its overall journey through the supply chain before completing product purchase by using a DL-Tags enabled mobile application to scan a Smart Tag.

The paper contributes an original and practical solution for verifiable supply chain management based on IoT and DLT which prevents counterfeit goods to be sold as originals, while the involved stakeholders have no need to expose their identity and business-related data to third parties. Stakeholders share product-related data solely directly, as product exchanges occur on the supply chain, and control the flow of data without the need for a trusted third party. A public ledger serves here as an intermediary providing *proof of existence* for significant events occurring on the supply chain, meaning that only data hashes based on actual product-related data exchanges are stored on the ledger. By using proofs of existence, the integrity of the actual data can easily be verified. The implemented solution is designed to be *agnostic of a DLT platform* used in the actual implementation, while the shared data format can be adapted to a specific use case. The solution is tested in the *TagItWine* use case, where wine bottles labeled by TIS Smart Tags are physically transferred between stakeholders, while the Ethereum blockchain serves as a trustless intermediary between them. Finally, we report a cost analysis of the implemented solution on the Ethereum blockchain that would need to be paid by the stakeholders. The largest expense relates to the product creation function which is paid by a producer, while all functions require much less gas. In December 2018, a producer would pay around 5 USD for logging a product creation event on the Ethereum chain, which is acceptable for high end products, while other functions cost in the range from 0.001 to 0.3 USD, which should be acceptable for other involved stakeholders. Note that all readings from the blockchain do not incur additional cost, and thus product verification by consumers is free of charge.

The paper is organized in the following way: Section II provides an overview of DLT, while relevant solutions combining IoT and DLT for supply chain management are analyzed in Section III. The benefits and requirements of the DL-Tags solution are introduced in Section IV. Technical details regarding the DL-Tags architecture and design are given in Section V. Our specific use case depicting a concrete application of DL-Tags is presented in Section VI, while the cost incurred by the solution is analyzed in Section VII. Section VIII concludes the paper and identifies directions for further work.

II. DISTRIBUTED LEDGER TECHNOLOGY

DLT enables the maintenance of a global, append only, data structure by a set of mutually untrusted participants in a distributed environment [6]. The most notable features of distributed ledgers are immutability, resistance to censorship, decentralized maintenance, and elimination of the need for a centralized trusted third party, i.e., *disintermediation*. In other words, there is no need for an entity to be in charge of conflict resolution and upkeep of a global truth that is trusted by all stakeholders who do not trust each other. DLT is suitable for tracking the ownership of digital assets, and its most prominent application is the Bitcoin network [7]. However, DLT holds promise beyond mere cryptocurrency transfer since an entry in the ledger may be generalized to hold arbitrary data.

A digital ledger stores transactions in an open ledger which holds a global state. Transactions serve as inputs that cause the change to the state, hence the ledger can generally be regarded as a transaction-based state machine. Different data structures exist for maintaining the ledger. One of such specializations of DLT, which is currently well-covered in literature and often used as a synonym for DLT is the blockchain data structure [8]. Since blockchain-based implementations of digital ledgers are the most mature at the moment, we are using the Ethereum blockchain for the implementation of the DL-Tags solution. Bitcoin [9] and Ethereum [10] are examples of stable reference blockchain implementations. New blockchain solutions are introduced, such as EOS, but during the DL-Tags development phase it was unstable and without adequate development tools.

Blockchain consists of ordered units called blocks that contain headers and transactions, as shown in Figure 1. Each block header, among other metadata, contains a reference

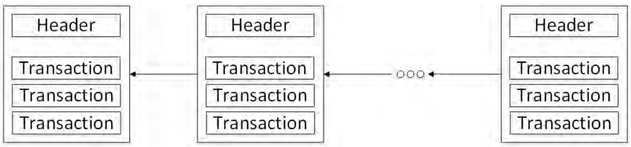

FIGURE 1. Blockchain as a data structure.

to its predecessor in the form of the predecessor's hash, which enables blockchain immutability. The initial state is hard-coded in the first block called the genesis block. Unlike other blocks, the genesis block has no predecessors.

Blockchain implementations can be public (*permissionless*) or private (*permissioned*). In a public and permissionless blockchain, each node can read from the ledger and append to the ledger. In a private and permissioned blockchain direct access to blockchain data and transactions submission is limited to a predefined list of authenticated entities [11]. Ledger maintenance in a private blockchain is performed by a trusted group of entities. Consequently, a user needs to trust these entities to behave honestly, which makes private blockchain environments trusted. In this project we require that all stakeholders and consumers of a certain product are able to read blockchain entries. Since the number of end consumers of a certain product type could be quite large, creating a predefined list of entities would be unattainable. Furthermore, we strive to develop a solution for a trustless environment eliminating the need for a trusted third party. Therefore, we consider only public blockchains, such as Bitcoin and Ethereum, to be adequate for the requirements of the DL-Tags project.

Blocks in a public and permissionless blockchain can be malicious and cannot be implicitly trusted. Consequently, consensus about each entry needs to be reached in the network. This consensus is basically an agreement about what is to be appended to the ledger by all nodes. Transactions are checked for validity by all nodes according to the protocol rules. The assumption is that a majority of nodes are honest and reliable. Both Bitcoin [9] and Ethereum [12] are based on the *Nakamoto consensus* which relies on a lottery function to elect the next node that will be able to append a block of transactions to the ledger. The elected leader broadcasts the new entry to the rest of the participants who implicitly vote to accept the entry by adding it to their local copy of the ledger, and may propose subsequent transaction entries that build on the ledger. In particular, the reference implementations are based on the lottery function called the *Proof of Work* (PoW).

The leader in the network based upon PoW becomes the first participant to successfully solve a cryptographic puzzle. For example, Bitcoin uses partial hash inversion as the cryptographic puzzle function. Partial hash inversion requires that the hash of a block of transactions together with a *nonce* (a free variable in the function) matches a certain pattern. The pattern starts with at least a predefined number of 0 bits. The function is intentionally difficult to solve since to manipulate the ledger, an attacker would need to have the supermajority of the computing power in the network, which makes an attack expensive to perform. Nodes that generate blocks in a PoW driven systems are called miners and the process is called mining. For the use of their resources, miners are granted tokens in the network as an economic incentive to mine (e.g., Ether in Ethereum, Bitcoin in Bitcoin). If there are no miners, no blocks can be mined and there is no transaction throughput.

Blockchain implementation Ethereum [10], [12] can hold arbitrary data in its transactions by offering a possibility to implement *Smart Contracts*. Smart contracts are distributed applications executed on the blockchain that support customized data storage and arbitrary business logic based on user needs, and are usually referred to as Distributed Applications (DApps). Smart Contracts expand the blockchain potential to become a decentralized platform rather than only a cryptocurrency. Since customized data storage is needed for implementation of the DL-Tags solution, Ethereum is chosen as the adequate blockchain implementation.

One of the most relevant issues hindering global-scale DLT adoption is its scalability. In PoW driven systems, a block is created every time a PoW puzzle is solved, thus transaction rate is limited by the periodicity at which blocks are created as well as transaction and block size. When increasing the number of nodes in the system, the frequency of block creation does not increase significantly due to the fact that the PoW puzzle difficulty is dynamic to enable convergence of block generation time to a fixed value. In Ethereum, a block is mined roughly every 15 seconds with a dynamic block size measured in *gas*, a unit to measure the fees required for a particular computation [12]. This value is dynamic and adapts to network conditions. This feature enables Ethereum's transaction rate to be roughly between 7 and 15 transactions per seconds. The process of storing information on the Ethereum blockchain with great certainty can last for a couple of minutes, while reading from the blockchain is executed in real time [8]. In the DL-Tags solution, only stakeholders are required to write on the ledger, while end consumers will only need to read information from the blockchain, which can be done in real time and free of charge, without deteriorating user experience.

III. RELATED WORK: APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

The most popular and widely known application of blockchain technology is the decentralized peer-to-peer digital currency Bitcoin [13] which takes advantage of blockchain's security, immutability, transparency, and ability to cut out the middleman. The main incentive for blockchain usage is its ability to cut the costs of legacy systems and manage increasing regulation requirements by taking advantage of the transparent nature of the technology. Startups are using private ledgers to cut the cost and time of settling transactions, while regulators are interested in the technology since its transparency and integrity allow market activity to be monitored in real time.

The use of blockchain is extensively considered in the IoT domain where daily objects interact with their environment to collect information and automate certain tasks. This vision requires, among other things, features that can be enabled by blockchain since IoT solutions involve multiple stakeholders in largely-distributed environments. These features include seamless authentication, data privacy, security, robustness against attacks, easy deployment, and self-maintenance [14]. Blockchains can be applied in different IoT areas [2], e.g., sensing, data storage, identity management, timestamping services, smart living applications, intelligent transportation systems, wearables, supply chain management, mobile crowd sensing, cyber law, and security in mission-critical scenarios. In IoT device management it can keep sensitive data private and ensure fine-grained access control based on time and user attributes [15]. According to Christidis et al. [16], the benefits of blockchain and IoT combination are in the following: Firstly, it facilitates the sharing of services and resources leading to the creation of service marketplace spanning multiple domains. Secondly, it allows automation of several existing and time-consuming workflows in a cryptographically verifiable manner.

The supply chain and logistics domain can take advantage of blockchain technology for product tracking, product tracing, or to trace related financial transactions [17]. Product tracking is applicable for cargo management or loading. Sharing cargo movement data between stakeholders can facilitate scheduling changes or handling of errors during cargo handling. Product tracing applications enable checking the authenticity of a product. The usage of blockchain for financial transactions tracing enables faster payments, lowers the transaction costs and mitigates fraud risks.

When considering the usage of blockchain, the developers should decide if the following features are necessary for their applications [14]. Firstly, if multiple copies of the ledger are not required and not needed to be distributed on multiple computers, traditional databases should be sufficient. Secondly, if all involved entities trust each other, traditional databases should suffice as well. If entities do not trust each other, but would trust a third party, the trusted party can manage their data (e.g., a bank or government). The usage of Blockchain as an intermediary should be considered in all other cases.

The DL-Tags solution presented in this paper focuses on the usage of blockchain in supply chain management under the assumption of a trustless environment. More precisely, it enables product tracing and allows all the stakeholders in a product lifecycle to validate a product they are handling and exchanging. Solutions related or similar to DL-Tags exist, such as a solution by Tian [18]. The paper recognizes the issue of centralized traceability systems and implements a food supply chain traceability system for real-time food tracing based on Hazard Analysis and Critical Control Points that is based on blockchain and IoT. The solution relies on IoT technologies (RFID, WSN, GPS etc.) for data collection, and stores product related data in the BigchainDB, which is a private decentralized data storage layer. It offers no economic incentives for ledger upkeep [19] and as such differs from DL-Tags which uses a public and trustless ledger. Another difference is that all users in the system are required to have a digital identity on the ledger.

Another relevant solution which tracks medical products and their surrounding temperature is presented in [20]. In contrast to DL-Tags, the proposed architecture is not DLT agnostic and does not focus on tracking product exchanges, but rather tracks temperature deviations in products' environments.

An innovative solution which proposes and implements a protocol for supply chains based on blockchain is presented by OriginTrail [21]. DL-Tags solves a subset of problems which are covered by OriginTrail; however, the latter relies on a custom token economy that introduces further complexity in the developed system, whereas DL-Tags does not rely on a custom token and thus introduces simplified procedures compared to OriginTrail.

IV. DL-TAGS SOLUTION

DL-Tags offers a decentralized, privacy-preserving and verifiable management of Smart Tags issued by TIS. It designs and develops a solution where Smart Tags information is shared directly between the involved stakeholders, using the interoperable infrastructure provided by the TIS system. DL-Tags extends the TIS solution by using blockchain technology, where blockchain represents an intermediary interceding the data exchange process between involved stakeholders to ensure data authenticity and integrity. Each interaction between stakeholders during the product item exchange is stored (logged) on the blockchain. Thus, stakeholders need to reach a consensus on product authenticity, while privacy is ensured by not storing human-readable information about product items on a public blockchain; only a product item information digest created by applying a cryptographic hash function is stored on the blockchain. This in turn greatly reduces the amount of data that needs to be stored on the blockchain as the information size is limited by the digest length. A blockchain entry is pseudo-anonymous since it discloses the identifier (usually in the form of an *address* on the ledger) of the entity responsible for creation of the entry, but the entry itself cannot be deciphered.

The goal of the DL-Tags solution is to disable situations where any of the involved stakeholders may attempt to attack the TIS system by propagating fraudulent or damaged products marked by Smart Tags under false pretenses. In particular, four specific challenges are solved by the DL-Tags solution:

1) manipulation of existing Smart Tags data;
2) duplication (cloning) and reuse of existing Smart Tags;
3) ambiguous chain of responsibility when a product is paid for, but never delivered, sent but never acknowledged upon delivery, damaged etc.;
4) circumvention of the entire TIS system by the creation of non-authentic Smart Tags.

An example of Smart Tag manipulation is a situation when a fraudulent stakeholder tries to modify a QR code and to misdirect future product users to a phishing site circumventing thus the entire TIS system. An incentive for such behavior might be to sell a cheaper fake product as a more expensive, branded one. This type of attack has already been identified by the TIS consortium [22] as a potential system vulnerability. Figure 2 shows how DL-Tags can identify and disable such situations of a phishing site deployment.

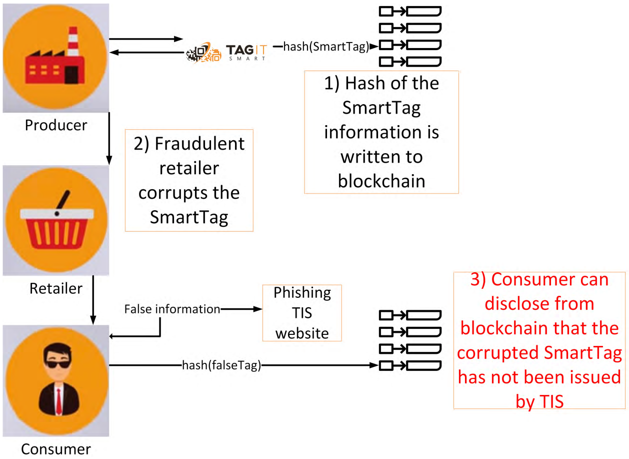
Producer
TAG IT SMART
hash(SmartTag)
1) Hash of the SmartTag information is written to blockchain
2) Fraudulent retailer corrupts the SmartTag
Retailer
False information
Phishing TIS website
3) Consumer can disclose from blockchain that the corrupted SmartTag has not been issued by TIS
hash(falseTag)
Consumer

FIGURE 2. Prevention of phishing site deployment.

Firstly, as in a regular TIS scenario, a producer requires the TIS system to issue a Smart Tag according to the provided product description. DL-Tags enhances this first step with additional interaction with a blockchain so that the information about Smart Tag creation is written to the blockchain. Secondly, a fraudulent retailer modifies the Smart Tag in order to sell a fake product as a branded one, and points a customer to a phishing site deployed to provide deceitful information about the product. Without using the DL-Tags solution, the consumer would scan the QR code and then be redirected to the phishing site providing deceitful information. However, by using the DL-Tags solution, a consumer can perceive, by analyzing blockchain entries, that TIS has not recorded the issuing of this particular Smart Tag. Thirdly, the consumer can conclude that the Smart Tag (i.e., product description) has been manipulated and stop the purchase.

An example of Smart Tag duplication which might arise during a product lifecycle is a situation when a fraudulent retailer duplicates Smart Tags of an expensive product and puts it on cheaper, lower quality products, as shown in Figure 3. Without using the DL-Tags solution, this fraudulent retailer would be able to distribute fake product items to other stakeholders or end consumers. Succeeding stakeholders or product consumers might eventually identify the problem by detecting multiple inquiries for this particular product item from the TIS system. However, it would be difficult to verify which stakeholder committed the deceit. This kind of fraud is prevented by the DL-Tags solution since all stakeholders using DL-Tags are enforced to disown a product when selling it. Therefore, they would not be able to forward products with duplicated Smart Tags regularly, since they can transfer ownership only for a single copy of the tag.

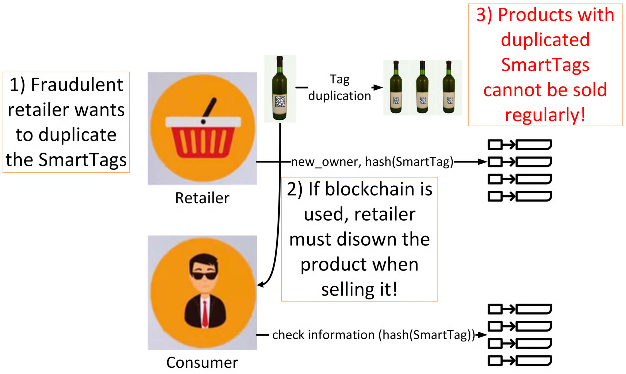
1) Fraudulent retailer wants to duplicate the SmartTags
Tag duplication
3) Products with duplicated SmartTags cannot be sold regularly!
Retailer
new_owner, hash(SmartTag)
2) If blockchain is used, retailer must disown the product when selling it!
Consumer
check information (hash(SmartTag))

FIGURE 3. Prevention of Smart Tag duplication.

Apart from phishing site deployment and Smart Tag duplication, a couple of other problems have been identified for which DL-Tags offers a straightforward solution. A stakeholder might sell a product to the next stakeholder, but without forwarding it physically. Afterwards, the buying stakeholder would end up without the bought product, while the selling stakeholder could assert having forwarded the product and could accuse the buying stakeholder of deception. The DL-Tags solution precludes such situations since the selling stakeholder needs to write on the blockchain that the product is sold, and the receiving shareholder needs to confirm the receipt of the product. If the received product is damaged or does not match the information provided in its Smart Tag, the receiving stakeholder can refuse to accept the delivered item and note such decision on the chain.

An additional problem might arise when a phishing TIS site is deployed and tries to issue Smart Tags with false information, defectively bypassing the entire TIS deployment. This situation can also be resolved by DL-Tags since each entity on the blockchain can be uniquely identified, as the majority of blockchain solutions relies on the public key infrastructure (PKI). Thus, each blockchain transaction is signed by the issuing entity, meaning that a fraudulent blockchain transaction upon product creation will not be signed by TIS.

For implementing the DL-Tags solution, we require the usage of a public and permissionless distributed ledger platform supporting Smart Contracts. Ethereum was chosen as the only stable solution which currently satisfies the listed requirements. Nonetheless, any other DLT that shares those properties can be used instead of Ethereum, which is known to exhibit scalability problems. We have excluded private chains from consideration since they require authentication of all users, which is inappropriate for TIS use cases with a large number of end consumers who are typically not users of private chains. Furthermore, private chains are implicitly trusted environments, while the focus of this project is on trustless environments.

The rest of this Section is organized as follows. System requirements are listed in Section IV-A, while sequence diagrams showing the main features and interactions between stakeholders are presented in Section IV-B.

A. SYSTEM REQUIREMENTS

The main requirements for the DL-Tags system are the following:

- The solution should be agnostic of the integrated distributed ledger platform; it should be possible to replace Ethereum with another distributed ledger platform with minor adjustments.
- The creation of Smart Tags by the TIS platform must be logged on the blockchain.
- After a stakeholder sells a product item, he/she must disown it.
- When a stakeholder receives the product item, he/she must confirm its authenticity and record this assertion on the blockchain.
- Each stakeholder should be able to unsubscribe to receive information about a product item after disowning it.
- Each stakeholder and consumer must be able to list all the blockchain entries for a specific product item which was under their possession.

B. SEQUENCE DIAGRAMS

Hereinafter, we assume the existence of three specific stakeholders, but the system is designed to scale to any number of potential stakeholders. The stakeholders are the following:

1) *TIS*: TagItSmart platform.
2) *Producer*: creator of a product item using Smart Tags provided by the TIS platform.
3) *E-commerce store*: retailer of a product item, i.e., an online store.

As a *consumer* consumes a product item in the end of its lifecycle, he/she is not regarded as a stakeholder, and thus does not need to have an account on the blockchain.

The basic building block of the DL-Tags solution is a function for storing transactions executed on the supply chain on a public blockchain. Initially, TIS must be able to store proofs of existence (digests) for newly created Smart Tags. Every product item has its *owner*. Each stakeholder needs to pass ownership of a product item when delivering it to the following stakeholder in the product item lifecycle. Consequently, every current owner can check previous owners of the product item. Each stakeholder needs to confirm the receipt of the product item using the description kept in its Smart Tag in the form of *voting*. A product item is considered *valid* only if all relevant stakeholders agree on its description. After passing ownership of a product item, stakeholders can receive information about any new stakeholder added to a specific product item, as well as other events in this product's lifecycle. This enables interested stakeholders to track handling information about their product items in the future. Stakeholders are given an option to unsubscribe or subscribe again to receive such information. Finally, consumers can check the validity of a product by reading that all stakeholders have *agreed* on a product's description. Figure 4 displays interactions between stakeholders of a product item. Interactions between the blockchain and stakeholders are presented as self-messages to simplify the diagram. These interactions include communication with DL-Tags proxy components introduced in Section V.

To enable product item tracking from the beginning of a product lifecycle, a producer needs to issue a request to the TIS platform for Smart Tag creation (message *requestTag*). TIS needs to store this transaction on the blockchain (message *1-createProductItem*). This step disables any fraudulent stakeholder to issue false Smart Tags. All transactions are signed using the private key of the entity issuing the transaction on the blockchain, meaning that no other entity can impersonate TIS on the blockchain if TIS private key is kept safe. Even if any fraudulent stakeholder issues a Smart Tag that might disclose false information, this would be easily observable on the blockchain since such transaction will not be signed by the private key possessed by TIS.

When a producer wants to pass a product item to another stakeholder (e.g., directly to a retailer, to a shipping company, etc.), it is necessary to issue a transaction to the blockchain along with the *id* of the next stakeholder in the product item lifecycle (messages *2a-addStakeholder and 2b-transferOwnership*). Upon receiving the product item physically, a new owner gets notified from the blockchain that he/she has been made a stakeholder and the owner of the product item at hand (messages *3a-addStakeholderNotif* and *3b-ownershipTransferredNotif*). The new owner can scan the Smart Tag on the received product and check if the provided information corresponds to the information stored on the blockchain. If there is a match, the new owners confirms Smart Tag validity by voting (message *4-vote*). Conversely, the new owner can check the previous records on the blockchain regarding this particular product item and ascertain which stakeholder has released the product item with a different Smart Tag.

All the stakeholders during product lifecycle need to store ownership transfer information on the blockchain when passing ownership of a product item, as well as confirmations that the Smart Tag information corresponds to blockchain entries upon receiving the product item.

When consumers buy the product, they have the option to check all previous transactions from the blockchain regarding a product item. This process is transparent to the consumer who uses a mobile application to check product authenticity, and the developed DApp handles all the checks. Consumers are in the end of the product lifecycle and are not granted ownership of a product item. Rather, the last owner disowns the product item by setting its owner to *none*. The reason for this is to alleviate each end consumer of a need to have an account on the blockchain. Upon receiving and scanning the

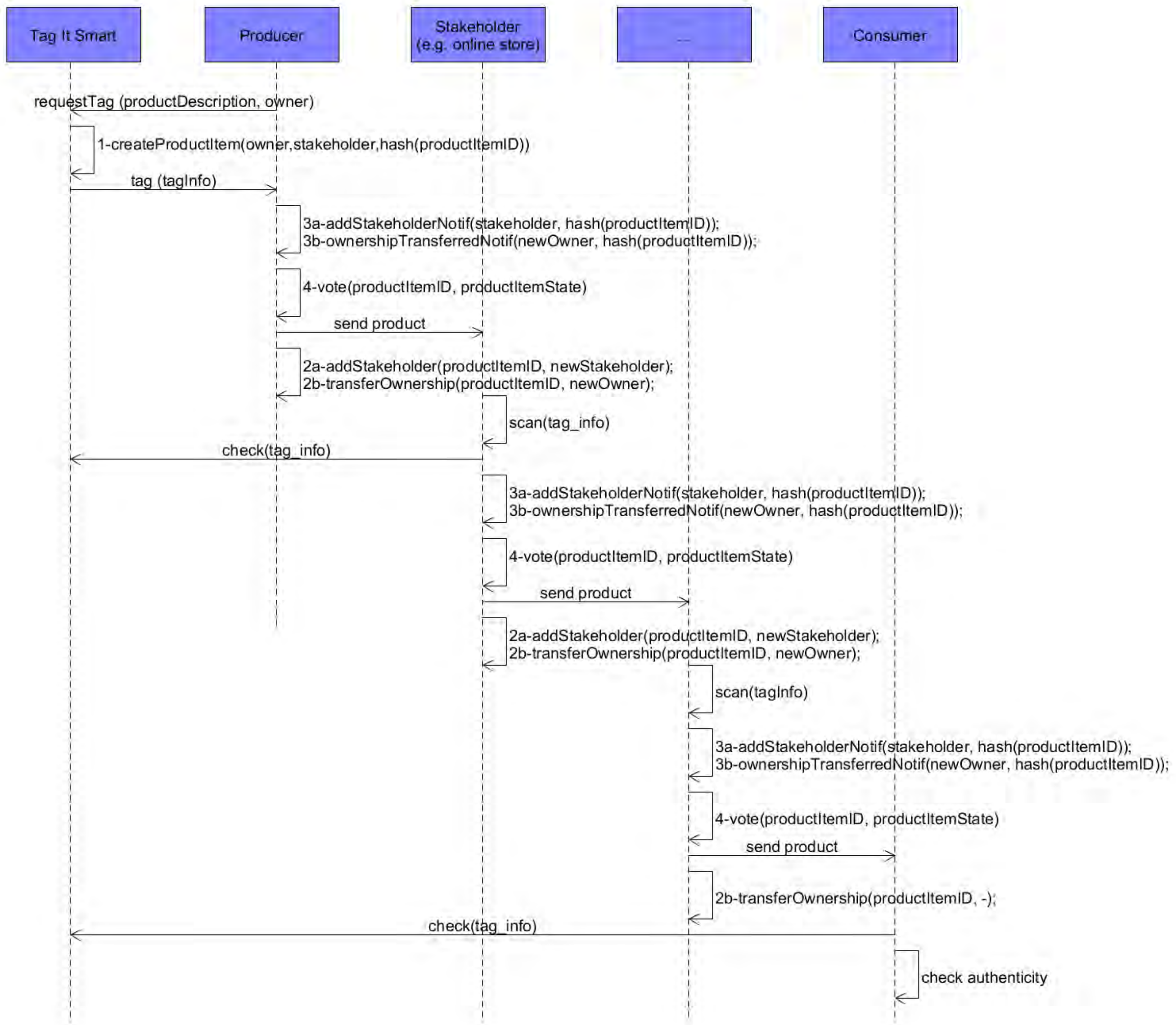
Tag It Smart
Producer
Stakeholder (e.g. online store)
...
Consumer
requestTag (productDescription, owner)
1-createProductItem(owner,stakeholder,hash(productItemID))
tag (tagInfo)
3a-addStakeholderNotif(stakeholder, hash(productItemID));
3b-ownershipTransferredNotif(newOwner, hash(productItemID));
4-vote(productItemID, productItemState)
send product
2a-addStakeholder(productItemID, newStakeholder);
2b-transferOwnership(productItemID, newOwner);
scan(tag_info)
check(tag_info)
3a-addStakeholderNotif(stakeholder, hash(productItemID));
3b-ownershipTransferredNotif(newOwner, hash(productItemID));
4-vote(productItemID, productItemState)
send product
2a-addStakeholder(productItemID, newStakeholder);
2b-transferOwnership(productItemID, newOwner);
scan(tagInfo)
3a-addStakeholderNotif(stakeholder, hash(productItemID));
3b-ownershipTransferredNotif(newOwner, hash(productItemID));
4-vote(productItemID, productItemState)
send product
2b-transferOwnership(productItemID, -);
check(tag_info)
check authenticity

FIGURE 4. Interactions between DL-Tags stakeholders.

product item, a consumer compares the blockchain entry for this product with the Smart Tag information and receives validation result, i.e., if the Smart Tag information has been stored on blockchain by previous stakeholders and if all stakeholders agree on its description. If not, consumers become aware of the irregularities during the product item lifecycle and can initiate product item return to the retailer.

V. DL-TAGS ARCHITECTURE

Each stakeholder (referred to as *Platform* in the following diagrams) needs to communicate with the blockchain. In the DL-Tags solution, a DL-Tags Proxy component is introduced that is responsible for handling all the interactions with the blockchain so that the stakeholders do not have to manage blockchain related messages on their own. Instead, stakeholders use the proxy's interface that is built upon *JSON RPC* (JavaScript Object Notation - Remote Procedure Call) to pass the data for storage on the blockchain.

A. COMPONENTS

The components and their interfaces are shown in Figure 6. The DL-Tags Proxy component specifies an interface to receive platform data, while *AMQP* (Advanced Message Queuing Protocol) is used to forward information back from the blockchain to Platforms. Interactions with the blockchain are technology specific, and a DL-Tags DApp, a set of Smart Contracts, is used to interact with the Ethereum blockchain in our implementation. However, the messages between a platform and the DL-Tags Proxy use a stable, technology

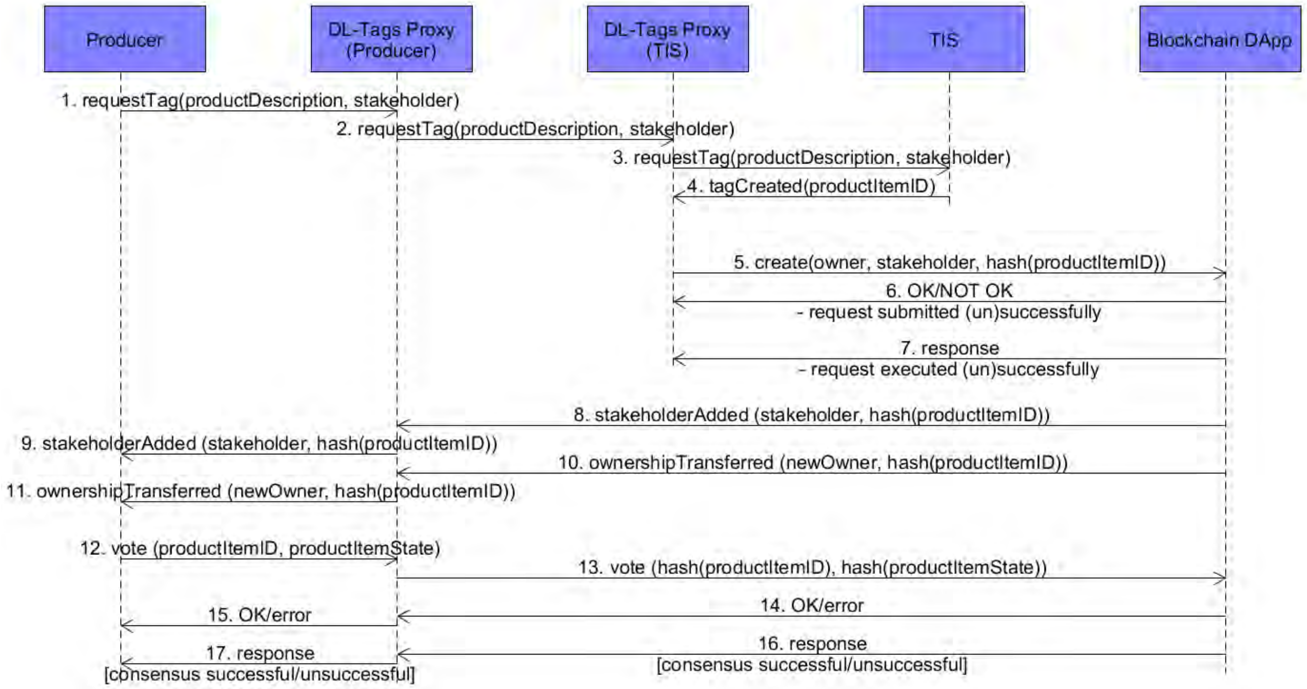
Producer
DL-Tags Proxy (Producer)
DL-Tags Proxy (TIS)
TIS
Blockchain DApp
1. requestTag(productDescription, stakeholder)
2. requestTag(productDescription, stakeholder)
3. requestTag(productDescription, stakeholder)
4. tagCreated(productItemID)
5. create(owner, stakeholder, hash(productItemID))
6. OK/NOT OK
- request submitted (un)successfully
7. response
- request executed (un)successfully
8. stakeholderAdded (stakeholder, hash(productItemID))
9. stakeholderAdded (stakeholder, hash(productItemID))
10. ownershipTransferred (newOwner, hash(productItemID))
11. ownershipTransferred (newOwner, hash(productItemID))
12. vote (productItemID, productItemState)
13. vote (hash(productItemID), hash(productItemState))
14. OK/error
15. OK/error
16. response
[consensus successful/unsuccessful]
17. response
[consensus successful/unsuccessful]

FIGURE 5. Create product.

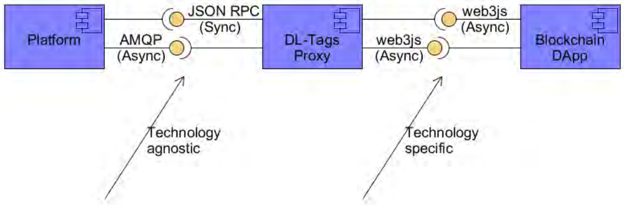

FIGURE 6. Interactions between stakeholders.

agnostic interface, and thus can be adapted seamlessly to integrate another digital ledger.

Each Platform needs to implement its own platform-dependent Platform Plugin, run a DL-Tags Proxy instance, download the blockchain and synchronize with the network.

B. FEATURES

Interactions with the blockchain previously shown in Figure 4 are presented in more detail in this Section by elaborating on the interactions between a platform and blockchain via the proxy. These features include: product creation (message *1-createProduct* from Figure 4), adding a stakeholder (message *2a-addStakeholder* from Figure 4), transferring ownership (message *2b-transferOwnership* from Figure 4), and receiving a stakeholder added notification (messages *3a-addStakeholderNotif* and *3b-ownershipTransferredNotif* from Figure 4). Information about product items available through Smart Tags is referred to as *productItemState* in Figures 5-9.

DL-Tags Proxy implements interfaces for execution of the aforementioned functionalities. DApp implements the same functionalities as DL-Tags Proxy on the blockchain and ensures that all the transactions related to product registration, ownership changes, and confirmations are written on the blockchain. Furthermore, it initiates announcements to the stakeholders when necessary, e.g., when a stakeholder is added or ownership of a product item has been transferred.

1) CREATE PRODUCT

Product creation is initiated by the producer and is shown in Figure 5. A request for Smart Tag creation is forwarded to TIS via DL-Tags Proxys of the producer and of the TIS system. Upon Smart Tag creation, DL-Tags Proxy of TIS sends a create request to the blockchain, adding TIS and the producer as stakeholders for the created product item representation. The producer is notified of being added as a stakeholder by its own DL-Tags Proxy. Afterwards, the producer is requested to vote on the validity of information stored on the Smart Tag.

2) ADD A STAKEHOLDER AND TRANSFER OWNERSHIP

When transferring a product item to another stakeholder, the current owner firstly needs to add the new stakeholder to the product item, and secondly transfer ownership of the product item to the added stakeholder. The procedure for adding a new stakeholder is shown in Figure 7. Messages 3 and 4 are generated by the DApp and sent to the stakeholder to confirm the receipt of the request. Messages 5 and 6 are asynchronous and will be placed in the invoker's queue. They serve to report that a request is recorded on the blockchain

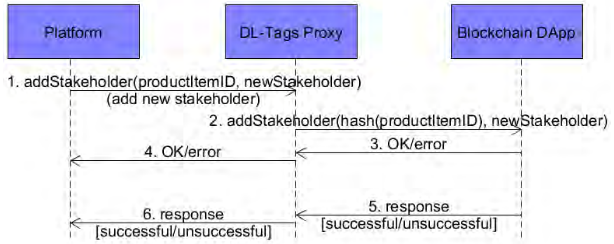
Platform
DL-Tags Proxy
Blockchain DApp
1. addStakeholder(productItemID, newStakeholder)
(add new stakeholder)
2. addStakeholder(hash(productItemID), newStakeholder)
3. OK/error
4. OK/error
5. response
[successful/unsuccessful]
6. response
[successful/unsuccessful]

FIGURE 7. Add stakeholder.

and the invoker can choose to act upon receipt. This is done to accommodate the long *time to first confirmation* (i.e. the time from the moment that the transaction has been issued up until the moment it has been included in a candidate block). The procedure for ownership transfer is similar, with the same parameters. Only a current product item owner is allowed to transfer ownership to another stakeholder.

3) NOTIFICATIONS FROM BLOCKCHAIN

When a stakeholder is added by one of the current product stakeholders, a notification is received from DApp, as shown in Figure 8. The new stakeholder needs to confirm the possession of the product. As seen in Figure 4, the new stakeholder scans the digital product, and confirm that the information associated with its Smart Tag corresponds to the current product item information stored on the blockchain. This is recorded on the blockchain by voting. Each stakeholder needs to vote on product item validity after being added as a new stakeholder. When a stakeholder is added as the new owner, he/she is notified via an event fired by the blockchain.

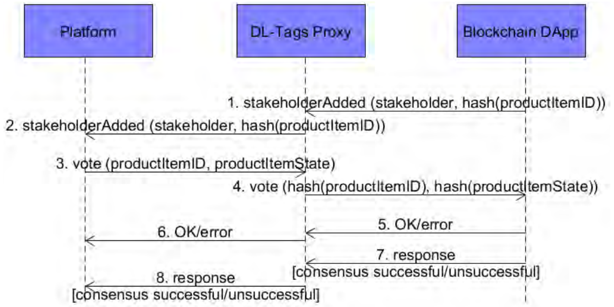
Platform
DL-Tags Proxy
Blockchain DApp
1. stakeholderAdded (stakeholder, hash(productItemID))
2. stakeholderAdded (stakeholder, hash(productItemID))
3. vote (productItemID, productItemState)
4. vote (hash(productItemID), hash(productItemState))
5. OK/error
6. OK/error
7. response
[consensus successful/unsuccessful]
8. response
[consensus successful/unsuccessful]

FIGURE 8. Stakeholder added notification.

C. PRODUCT STATUS CHECK

Each product stakeholder and its consumer can check the product's status on the blockchain. This is performed by sending a check message to the DL-Tags Proxy which is then forwarded to the blockchain DApp, as shown in Figure 9. In its simplest form, the DApp responds if everything is in order with the product item or not. In the former case all the previous stakeholders have confirmed product validity during voting, while in the later case not all stakeholders agree on product validity.

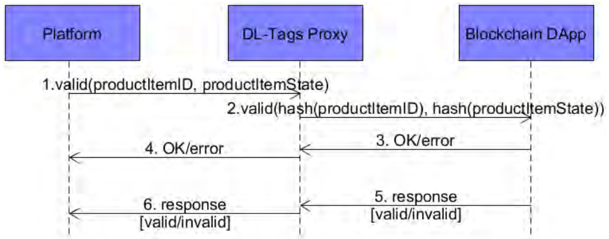

FIGURE 9. Product validation check.

VI. USE CASE SCENARIO

The DL-Tags solution has been implemented and tested in the framework of the TagItWine use case[1] where wine bottles become digital products. Our main goal is to ensure brand protection and track the lifecycle of a bottle of wine from a winery to an end consumer via an e-commerce store.

The specific stakeholders addressed by the DL-Tags solution in the TagItWine use case are shown in Figure 10. The first stakeholder is a producer, i.e., winery in our specific use case. The product is then transferred to a retailer. Magento, an open source e-commerce platform, is deployed as a retailer in our use case. The provider of a Magento e-commerce store is supposed to acquire the product from the producer, check its authenticity, and offer it to potential buyers. Consumers, using the Magento e-commerce store, are able to find the product online and perform a purchase. When the product is delivered, consumers can check its authenticity by using the TagItWine mobile application.

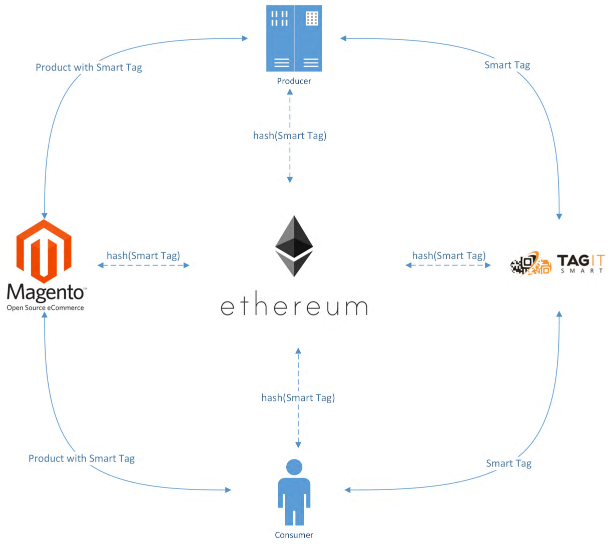

FIGURE 10. Stakeholders in DL-Tags use case.

The following applications have been deployed to demonstrate the usability of the DL-Tags solution:

- Producer application: its interface enables product creation, voting on Smart Tag information genuineness, and ownership transfer. The application has been

[1] https://www.tagitwine.me/

deployed and integrated with its respective DL-Tags Proxy instance.

- Magento e-commerce store: a dedicated interface has been deployed in Magento e-commerce platform allowing observation and validation of incoming products. The application has been integrated with its respective DL-Tags Proxy instance. The products are made available to consumers through e-commerce store only upon successful validation by e-commerce store provider. Additionally, the deployed interface allows Magento store provider to disown the product.
- Consumer application: allows checking the product validity by using the TagItWine mobile application. The TagItWine application has been integrated with its respective DL-Tags Proxy instance.

VII. COST EVALUATION

This section analyzes cost approximations for method invocations defined in the DL-Tags solution. The costs are declared in Ether and in USD. An operation on top of the Ethereum blockchain is paid in *gas*. The amount of gas used for each DL-Tags method invocation is shown in Figure 11. Apart from methods, the amount of gas is also presented for initial contract deployment. The largest amount of gas is required for product creation (1478198). The reason for such high gas cost is due to the fact that this action executes substantially more write operations on the blockchain. Generally, write operations are the most expensive operations on Ethereum in terms of gas cost. Initial contract deployment requires 41.64% less gas compared to product creation. All other methods require much less gas. Transfer of ownership requires the least amount of gas, only 14649. To add a new stakeholder 63599 gas is needed, while voting requires 89603 of gas.

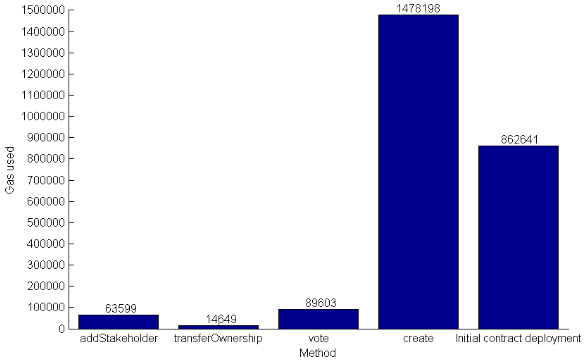

FIGURE 11. Gas used per method invocation.

A stakeholder can declare how much *wei* (1 Ether = 10^{18} wei) he/she is willing to pay per unit of gas for a specific transaction. Depending on the offered amount of wei for a transaction, a miner might decide to include this transaction in a block. In other words, the more stakeholders pay, the more probable it is that their transaction will be included in a candidate block faster. The values shown in Figure 12 show the changes of price per each method invocation in Ether during year 2018. The values are calculated using the average gas price that users were willing to pay for a transaction in a given period.[2] Herein, we assume that an average gas price implies block inclusion time below 400 seconds (with no guarantees). By using the ratio between any fiat currency, that is declared legal tender by a government but has no intrinsic or fixed value and is not backed by any tangible asset (USD, EUR, etc.), and Ether at that given period, we can calculate how much a transaction actually costs.[3] The cost in USD is shown in Figure 13.

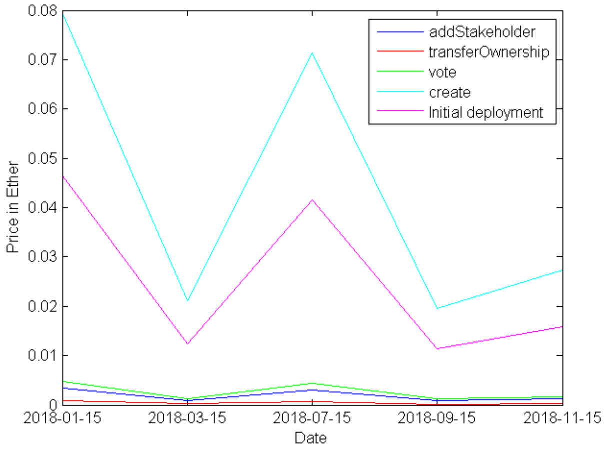

FIGURE 12. Method invocation price in Ether.

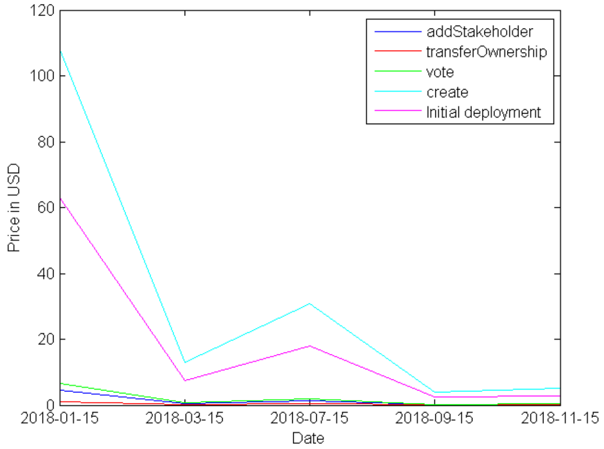

FIGURE 13. Method invocation price in USD.

The price for DL-Tags method invocation in USD was volatile during the year 2018 due to the volatile ETH/USD ratio. Product creation would cost 108 USD in January, while in December the cost would be around 5 USD. The price in December is acceptable for higher end products, while the price in January could hardly be acceptable for any consumer product. The cost of other methods is much lower since they

[2] https://etherscan.io/chart/gasprice

[3] https://ethereumprice.org/

require less gas. In November, the *addStakeholder* invocation would cost 0.001 USD, *transferOwnership* would cost 0.049 USD, while *vote* would cost 0.3 USD, which is quite reasonable.

VIII. CONCLUSION

The DL-Tags solution presented in this paper enables decentralized, privacy preserving and verifiable management of products labeled with Smart Tags. It is based on the permissionless and public Ethereum blockchain. DL-Tags offers a mechanism for unilateral consensus in supply chain management. All the stakeholders need to agree on information available through Smart Tags. End consumers can rest assured they are consuming the product as declared on the Smart Tag.

A use case is presented ensuring brand protection and anti-counterfeiting in wine industry. The use case involves handling a product item from its producer via an e-commerce store provider to the end consumer. Magento e-commerce store was used in our specific use case. DL-Tags architecture and its DL-Tags Proxy component allow for smooth integration with the stakeholder systems without the need to know blockchain implementation details. Furthermore, the DL-Tags architecture is adaptive and can be integrated with other blockchain solutions without the need for any adjustments in the stakeholder systems.

Cost approximations for invocation of methods in the DL-Tags use case were conducted. They revealed that the cost of using the Ethereum blockchain (without initial contract deployment) varied from 4.83 USD to 128.12 USD for analyzed periods during year 2018. The cost of initial contract deployment varied from 2.38 USD to 63.14 USD. The lower price of around 5 USD could be acceptable in a real-world scenario for higher end products, while the peak price of 128 USD would probably prove to be too high.

The DL-Tags solution is distributed and decentralized, without a central node storing product exchange-related information. As such, it can spur further adoption of decentralized supply chain management solutions in which stakeholders have no need to share their business-related information to third parties, as in the prevailing centralized solutions which require a trusted intermediary. In cases when stakeholders are suspicious about a third party potentially misusing the acquired information for its own benefit and at the expense of others, DL-Tags enables the maintenance of confidential product item exchange-related information between a producer, e-commerce store and an end consumer without disclosing this information to stakeholders outside the supply chain.

In terms of future work we are investigating the *closed loop supply chains* [23] that are emerging in the context of *circular economy* which promotes sustainable flows of products and materials which are being reused. Circular economy is restorative and regenerative by design to keep products, components and materials at the highest value and utility at all times [24]. The linear supply chain processes which are currently supported by DL-Tags would need to be revised to close the loops from waste to material rebuilt into a new product. We are confident that by reusing the principles presented in this paper adequate IoT- and DLT-based solutions supporting closed loop supply chains can be developed and deployed.

REFERENCES

[1] M. Christopher, "Logistics and supply chain management: Strategies for reducing cost and improving service (second edition)," *Int. J. Logistics Res. Appl.*, vol. 2, no. 1, pp. 103–104, 1999.

[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, to be published.

[3] S. Georgoulas, S. Krco, and R. van Kranenburg, "TagItSmart—SmartTags for unlocking business potential," *IEEE IoT Newslett.*, Nov. 2017. [Online]. Available: https://iot.ieee.org/newsletter/september-2017/tagitsmart-smarttags-for-unlocking-business-potential.html

[4] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2015, pp. 180–184.

[5] O. Svein, *Beyond Bitcoin Enabling Smart Government Using Blockchain Technology* (Lecture Notes in Computer Science), vol. 9820. Cham, Switzerland: Springer, 2016, pp. 253–264.

[6] A. Narayanan and J. Clark, "Bitcoin's academic pedigree," *Commun. Acm*, vol. 60, no. 12, pp. 36–45, 2017.

[7] P. Franco, *The Blockchain-Understanding Bitcoin*. New York, NY, USA: Wiley, 2014, pp. 95–122.

[8] F. M. Benčić and I. P. Žarko, "Distributed ledger technology: Blockchain compared to directed acyclic graph," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst.*, Jul. 2018, pp. 1569–1570.

[9] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008, p. 9. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, 2014. [Online]. Available: https://blockchainlab.com

[11] B. Group and J. Garzik, *Public Versus Private Blockchains. Part 1: Permissionless Blockchains*. Washington, DC, USA: Bitfury Group, 2015, pp. 1–23.

[12] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum & Ethcore, Ethereum Project Yellow Paper 151, 2014, pp. 1–32.

[13] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[14] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[15] Q. He, Y. Xu, Z. Liu, J. He, Y. Sun, and R. Zhang, "A privacy-preserving Internet of Things device management scheme based on blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 11, pp. 1–12, 2018.

[16] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[17] M. Petersen, N. Hackius, and B. von See, "Mapping the sea of opportunities: Blockchain in supply chain and logistics," *Inf. Technol.*, vol. 60, nos. 5–6, pp. 263–271, 2018.

[18] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2017, pp. 1–6.

[19] *How BigchainDB is Immutable—BigchainDB Documentation*. Accessed: Dec. 14, 2018. [Online]. Available: http://docs.bigchaindb.com/en/latest/immutable.html

[20] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.

[21] B. Rakic, T. Levak, Z. Drev, S. Savic, and A. Veljkovic, "First purpose built protocol for supply chains based on blockchain," OriginTrail, Ljubljana, Slovenia, Tech. Rep. 1, 2017. [Online]. Available: www.origintrail.io

[22] TagItSmart consortium, *D2.3-Final Enabler for Funcodes*, Project Deliverable, Feb. 2018.

[23] R. De Angelis, M. Howard, and J. Miemczyk, "Supply chain management and the circular economy: Towards the circular supply chain," *Prod. Planning Control*, vol. 29, no. 6, pp. 425–437, 2018.

[24] I. Askoxylakis, "A framework for pairing circular economy and the Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

FEDERICO MATTEO BENČIĆ received the M.Sc. degree in information and communication technology from the Faculty of Electrical Engineering and Computing, University of Zagreb, in 2017, where he is currently pursuing the Ph.D. degree with the Department of Telecommunications. He was a Guest Student with the Faculdade de Engenharia da Universidadedo Porto, University of Porto, in 2015. He is currently an Assistant Professor with the Department of Telecommunications, Faculty of Electrical Engineering and Computing, University of Zagreb. His research interest includes the applications of distributed ledger technology in the Internet of Things area.

PAVLE SKOČIR received the B.Sc., M.Sc., and Ph.D. degrees in computing and information and communication technology from UNIZG-FER, in 2010, 2012, and 2018, respectively.

He is currently a Research Assistant with the Internet of Things Laboratory (IoTLab@UNIZG-FER), Faculty of Electrical Engineering and Computing, University of Zagreb. He has participated in six research projects supported by international and national foundations and programmes or in cooperation with private companies. He has coauthored 23 papers, and he has presented his research at 13 conferences in eight different countries. His research interest includes the Internet of Things (IoT). The focus of his research is on energy efficient execution of intelligent tasks on sensor nodes, achieving interoperability between the IoT platforms, and on applying blockchain technology in the IoT area. He is a member of the IEEE Communications and Computer Societies. He has served as the Chair of the IEEE Computer Society Chapter within the IEEE Student Branch, University of Zagreb.

IVANA PODNAR ŽARKO received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from UNIZG-FER, in 1996, 1999, and 2004, respectively. She is currently a Full Professor with the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia (UNIZG-FER), where she teaches distributed information systems. She has been with the Department of Telecommunications, UNIZG-FER, since 1997, where she is currently leading the Internet of Things Laboratory. She was a Guest Researcher and a Research Associate with the Technical University of Vienna, Austria, and a Postdoctoral Researcher with the Swiss Federal Institute of Technology, Lausanne (EPFL), Switzerland. She was promoted to a Full Professor, in 2017. She has participated in a number of research projects supported by national sources and EU funds. She is currently the Technical Manager of the H2020 Project Symbiote: Symbiosis of Smart Objects Across IoT Environments. She is currently participating in the Centre of Research Excellence for Data Science and Advanced Cooperative Systems, which is the first National Center for Excellence in the field of technical sciences in Croatia. She has coauthored more than 60 scientific journal and conference papers in the area of large-scale distributed systems, the IoT, and big data processing. She is a program committee member of a number of international conferences and workshops. She was the Chapter Chair of the IEEE Communications Society, Croatia Chapter, from 2011 to 2014. She has received the award for engineering excellence from the IEEE Croatia Section, in 2013.