Tamper-Proof Volume Tracking in Supply Chains with Smart Contracts

Ulrich Gallersdörfer(✉) and Florian Matthes

Technical University Munich, Arcisstraße 21, 80333 Munich, Germany
ulrich.gallersdoerfer@tum.de

Abstract. Complex supply chains involve many different stakeholders such as producers, traders, manufacturers, and consumers. These entities comprise companies and other stakeholders spanning different countries or continents. Depending on the involved goods, the origin and the responsible harvesting of these elements are essential. Due to their high complexity, these systems enable the introduction of resources with forged identity, tricking the participants of the supply chain into believing that they acquire goods with specific properties, e.g., environmentally friendly wood or resources which are not the result of child labor. We derive requirements from the global world trade of timber and timer-based products, in which the origin of a large portion of certified wood cannot be verified. A set of smart contracts deployed within the Ethereum platform allows for a transparent supply chain with validated sources. The platform enables the tracking of variations of the original good, tracing not only the raw material but also the resulting products. The proposed solution introduces a novel exchange contract and ensures a correct overall volume of assets managed in the supply chain.

Keywords: Blockchain · Volume tracking · Ethereum
Smart contracts · Supply chain · Logistics

1 Introduction

The manufacturing of products of daily use such as furniture or work material is the result of complex supply chains, involving multiple steps of different entities in the respective systems. Usually, mining facilities produce the raw materials for these products. These entities sell the resource, either with or without intermediaries to other manufacturers which purify the raw materials or create base components for further value creation. The process is repeated for each manufacturing step until a final product is being sold to end-customers. These procedures are time-consuming and tedious as a large number of stakeholders is involved [19].

Customers have high demands on products of their desire [4]. Not only should the product satisfy their needs in terms of functionality, design or appearance, but also the production should only involve environmentally friendly components and must avoid exploitation of child labor or unreasonably low wages [11].

G. Mencagli et al. (Eds.): Euro-Par 2018 Workshops, LNCS 11339, pp. 367–378, 2019.
https://doi.org/10.1007/978-3-030-10549-5_29

If their desires are satisfied, the willingness to pay for these products increases [17]. However, these requirements pose difficulties for some manufacturers. Due to their extensive network of suppliers, they often cannot verify the information they receive about incoming resources, leaving them unaware of any manipulations, fraud, or mislabeling [7]. As their customers are willing to pay more for environmentally sound products, they have an intrinsic interest in the production of such assets and therefore in a method to trace the origin of their base materials.

Other entities involved in the process also have an interest in removing fraudulent entities in the supply chain. Honest producers of base resources suffer from the introduction of intentionally mis-labeled goods on the market. Independent of the demand, a decrease of the overall supply could lead to higher market prices, increasing the profits of the original producers. Also, the society emphasizes the importance of environmentally sound and employee-friendly manufacturing and production of goods [3].

Blockchain technology promises to solve problems in the supply-chain industry [9]. A Blockchain network consists out of many interconnected computers which share a common state of a ledger [16]. The entities in the system define the rules for changing the state and appending new information to the ledger. As of the absence of a central entity, there is no way to forge or delete information afterward. As of these properties, the system can be used for creating decentralized currencies like Bitcoin [12] or individual Smart Contracts with platforms like Ethereum [20]. These contracts are software programs which are deployed and executed on the Blockchain. After the deployment, these contracts cannot be changed, assuring their integrity.

Many companies consider individual Smart Contracts as an opportunity to digitize supply chains and the involved goods. Companies such as Maersk [5] have already created concepts of Smart Contracts to trace the contents and ownership of containers transported by ships. These proposals focus on the digitalization of business processes, like the digitalization of the receipt of ownership, which does not fit with the above-stated problem. Other approaches like Everledger [10] do not cover the possibility of a good to be manipulated. We derive our requirements and goals of a use case we describe in following.

The supply chain we consider includes the group of enterprises and companies which harvest, trade and process resources made of wood from forests from different countries. The aim of the supply chain is the production of goods such as furniture or charcoal, generally speaking everything that can be made out of wood. Wood itself is often certified by authorities (such as the UN [14]) or NGOs (such as NEPCon [13]) which ensure that the wood originates from sustainable forests. In theory, these certifications ensure that only sustainable wood enters the supply chain. However, the chain itself is highly complex: Many different stakeholders are involved, the trading routes are opaque and it is very difficult to keep track of the flow of goods. The origin of the base resource wood is often non-transparent or fabricated, leaving manufacturers in the dark about the materials they use. Malicious entities in the system use these factors to introduce wood into the system without the required certification. This leads to a higher overall output of certified wood in contrast to the lower maximum volume that is allowed to be produced. Studies show that the volume of uncertified wood from certain regions increased over 50% [6]. This increased volume is the main problem in the supply chain. We derive our requirements from this specific case for our system.

One other paper gives a sound overview about the problem in timber tracking and discusses these issues [2]. The authors propose a Blockchain-based solution, writing each transportation operation in the Blockchain. They also outline possible limiting factors regarding the technology.

In this paper we propose a smart contract system enabling the participants of a supply chain to agree on

- the entities that are allowed to take part in the system
- the specification of the resources, products or goods handled on the supply chain
- the exchange rate between two types of resources
- how entities are selected for issuing new resources

while ensuring that

- no party can create a token/good if it has not the right to
- no resource, product or good can be spent twice
- the overall created volume remains the same when handed through the supply chain.

The system is implemented with Solidity for the platform Ethereum. We are confident that implementations in any other Blockchain platform supporting smart contracts are feasible, as the theoretical considerations remain constant.

After describing the various problems of the selected supply chain in detail in Sect. 2, we introduce the design of the system including the users and smart contracts involved in Sect. 3. We further discuss the processes and propose a bootstrapping mechanism. In Sect. 4 we discuss the limitations and the applicability of our proposed solution and end with an conclusion in Sect. 5.

2 Problem Statement

First, we introduce why a centralized approach under the supervision of NGOs or regulators is not feasible. Afterwards, common problems of traditional Blockchain-based solutions for supply chains are outlined. We describe the technical layout of the implementation, as it is important to understand the objective of the proposed solution.

2.1 Centralized Platform Issues

As there are already NGOs and governments in place that validate forest owners for a sustainable and environmentally-friendly approach, one might ask why these regulations do not prevent the introduction of mis-labeled materials? The problem is that only the producers itself are validated and the information provided by them can be validated very easily. Forests can be measured and an estimation gives a good indicator if the entity under validation is cheating. For intermediaries, this process is much harder, as the information itself can easily be tampered with without a convenient way to verify it. This imbalance leads to the possibility to introduce uncertified goods into the supply chain. Therefore, a digitalized system has to be put in place to track these streams and prevent the introduction of illegal resources.

A platform for a tamper-proof tracking and issuing of goods and resources is suited. However, it is the question if this platform should be run by a single entity or shared among all participants. There are different reasons against a centralized approach: The central authority is a worthwhile goal for attacks, as its shutdown paralyzes the system or renders the attacker able to manipulate account balances. These risks can be minimized, but one other issue remains: The missing trust in the central authority (CA) [8]. As there are many different entities which would qualify for this position, it would be impossible to agree on one entity because of the different interests of stakeholders. The CA could easily track every asset, could block single users or unilaterally introduce changes to the system. As of this, entities in the system are not interested in a centralized approach. As of that, we propose a decentralized system in which decisions are transparent.

2.2 Technical Issues

The overall goal is to propose a platform that enables to track assets and prove a valid origin. The platform is designed to be decentralized and governed only by its entities, however in many decentralized applications a proportion of centralism remains. A supply chain handles individual goods. Each and every asset transported in the supply chain could be identified by specific characteristics: Entities trace goods via serial number or specific material structures such as a DNA. However, these assumptions sometimes cannot be applied, as producers face different problems:

Combination of Different Goods. The combination or separation of goods leads, on a data level, to a creation of new good(s) and the destruction of old good(s). It is important to define the boundaries and rules for these processes, because if they are undefined, these procedure could lead to the creation of valid resources out of thin air on data level. Other questions arise: Which entity defines the new serial number of the defined product? Is it possible to sufficiently store all data associated with one single product, possibly comprising out of arbitrary amount of sub-products, goods and resources?

Loss of Information. In real world, the products or goods can lose the information that identifies them. This rarely happens to finished products at the end of manufacturing process, however it is possible that the association between two single goods (a base product and a manufactured product) gets lost as it is too costly to validate which base product was processed to a manufactured product. The information can also be lost as of the manufacturing process itself. Regular wood loses its DNA sequence when burned to produce coal. On a technical level, it is impossible to ensure the integrity of the information if the real-world processes are not sufficient to identify single entities.

Volume-Usage for Base Products. Manufacturers have reasons to not consider the single entity of a material (e.g. a tree), but measure the volume of these materials. They estimate their output for the given input volume, without tracking which entity winds up in which output. The complexity increases as base materials from different suppliers are combined, as it becomes impossible to refer the outputs to the resources of different suppliers. Additionally, the tracking is too costly to implement.

Entities of the system face another problem: All participants of the supply chain are required to use the platform for their transactions. If one user does not support the platform, the chain is interrupted. This leads to the fact that recipients of resources do not receive the equal amount on the platform.

3 System Design

In this section, we describe the design of the Blockchain-based supply chain network.

3.1 Entities

We identify all entities in the system by a regular Ethereum address. These addresses are either hashes of public keys or, in the case of smart contracts, random generated numbers. The owner of the identity also possesses the private key to express her will, in case of smart contracts code supplants the user. Therefore, we can store the identity about all involved entities or smart contracts with the data type `address`. In case the entity is a smart contract, the code decides upon the will of the address. Although both types of entities act in a similar way and have the same abilities, we separate between them for logical reasons. For clarity, we will refer to human entities as users and code entities as Smart Contracts (short: SC). An advantage of the equal treatment of entities in Ethereum is that the architects are able to replace users with Smart Contracts. A user has too many rights in SC A or one wants to impose a specific restriction for this specific user? One can create a SC B which replaces the user in SC A. The user is given the right to control SC B under the limits imposed in the code in SC B.

Users. First, we describe all human users in the system. As a general notice, we further refer to the goods represented on the Blockchain as tokens.

Regulators. The regulators are users in charge of validating all processes in the network. They can either be selected unilaterally by the entities deployed the system or can be selected via democratic processes within the system. We do not define any notion of how these regulators are selected or elected (as this varies between different supply chains), we define their tasks and responsibilities. Regulators select forest owners and validate their correct operation[1]. After a correct validation, they assign the right to create new tokens for a certain resource, either directly within the token contract or via a separate contract that regulates the amount of newly created tokens. Regulators also have the right to revoke access to the creation of new tokens if rules are violated. The regulators do not take part in the trade or exchange of tokens.

Trader. Traders are regular market participants in the supply chain. They are able to receive and send tokens they previously received. Their access to the system can be invitation only if necessary. We do not oppose any further restrictions to the traders in the system, as they do not have any rights to exchange tokens for other tokens or create new ones. The system designers can decide whether they want to include the traders in the democratic processes.

Creator of Goods. The producer is the creator of goods in the supply chain. She is responsible for creating new tokens and sending them alongside her real-world goods. Usually, a producer has the right to create only one type of good and therefore one type of token. Her rights to create tokens and the maximum specified amount per period depend on the decisions of the regulators. As her intrinsic motivation for a functional system, it is possible to involve the creator of the goods in the democratic processes of the system.

Manufacturer. The manufacturer has the same rights as the trader. However, she has the additional right to exchange one token for another at the exchange SC. The manufacturers are elected by a democratic process or are selected by other entities like the regulators. It is also possible to give traders and manufacturers the same rights, as we do not expect the trader to gain an advantage out of exchanging tokens for other tokens to which she has no real world product.

Smart Contracts. Further, we discuss the Smart Contracts specified in the system.

Central Authority Contract. In contrary to decentralized systems, our proposed solution contains a central authority SC controlling the system. As the governance of supply chains differ from industry to industry, we do not want to restrict the system to one specific design such as a majority vote. The owner of the contract, as mentioned before, can be replaced by any desired structure, i.e.

[1] Again, this process lies outside of the Blockchain and depends on the specific supply chain.

a democratic pattern or a 2 out-of 3 pattern. This decision has to be made by the architects of the specific implementation of the system. The central authority smart contract is the first contact in the system. It defines the available token and exchange contracts, is responsible for the selection of the regulators, and has the right to introduce new exchange rules or token contracts. It is also possible to deploy the contract in a way such that there is no governance afterwards possible; all rules and entities have to be agreed on before deployment on the Blockchain. Due to the transparency, the owner of the central authority contract can be reviewed by all participants of the system.

Tokens Contract. To enable compatibility with existing software components, the token contracts are modified ERC-20 token contracts [18]. ERC-20 SCs are widely accepted as they are mostly used in ICOs and other tokens on Ethereum. Our token SCs implement two additional functions: `createToken(uint amount)` and `modifyTokenAmount(address account, uint amount)`. The first function can only be executed by a producer or a regulated creation SC. It allows the creator of goods to create new tokens, because in ERC20 contracts the overall supply of the token is usually defined at the initialization of the contract. The second method is required for the exchange contract. The contract is responsible for the exchange of tokens, therefore reducing one amount on one contract and increasing the amount on another contract at the same time. The method allows the exchange SC to modify the balance of a single account. Besides the additional functionality, the token contract supports traditional methods as sending, checking account balances and sending amounts on behalf of another party.

Exchange Contract. The Exchange SC is the main contract for manufacturers which exchange their tokens for other tokens as they further processed the resources or created new products out of existing materials. The exchange SC is registered in the central authority contract and in all token contracts, otherwise it cannot manipulate the account balances in the existing token contracts. The contract also stores the exchange rates for pairs of tokens.

Regulated Creation Contract. The regulated creation SC is one example of a contract that regulates the usage of another contract, in this case a token contract and the right to arbitrary create new tokens of a producer. The user allowed to create new tokens is registered in the regulated creation contract, whereas the regulated creation contract is registered as an issuer in the token contract. In the regulated creation contract the regulators specify the maximum amount the user is allowed to issue, for example depending on their producing facility or other existing resources.

3.2 Processes

In this section, we describe recommended standard processes which occur while using the system.

Transfer of Goods. The transfer of goods is the basic process in the system. The system's main purpose is the transfer of goods on the Blockchain and is designed to be easy and comprehensible for every participant. The transfer of goods is facilitated in a regular way. The payment takes place with traditional arrangements such as bank transfer or cash. The shipment or transportation also happens in traditional ways. We do not create "digital twins" [1] on the Blockchain, as we do not want to track the individual component but rather the handled volume. A digital twin approach would be unnecessary, therefore the transfer of the digital good has to be executed manually. The sender just specifies the address of the receiver and the digital representatives are transfered. A easy rule applies: "If a good is bought and it is not accompanied with the same amount of the digital good, the good does not originate from a certified source." The transfer of goods is depicted in Fig. 1, in which malicious entities (red) are not able to introduce mis-labeled wood into the valid (green) supply chain. A red x marks where an operation fails on the Blockchain or in real world.

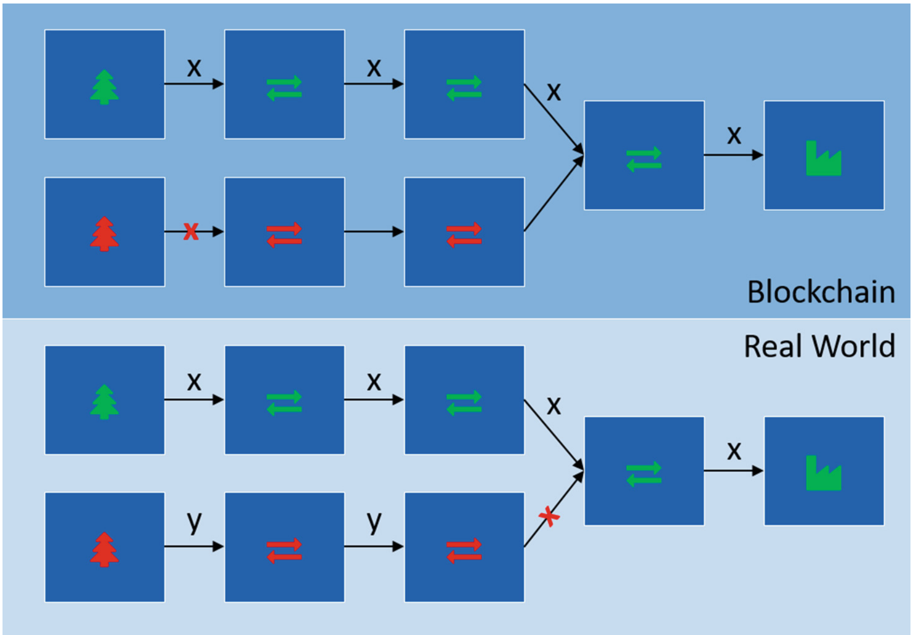

Fig. 1. Transfer of goods (Color figure online)

Exchange of Goods. The exchange of goods is a process required as the system supports many different digital goods. If a manufacturer wants to transform a good, she proceeds as always. The necessary physical steps stay identical. Additionally, she has to transform the digital good. To do so, she executes the method `exchange(uint Token1, uint token2)` to exchange one token for another. As of the atomic nature of the transaction, the exchange is either successful or aborts. It is not possible that the manufacturer keeps old tokens while creating new tokens or losing old tokens and not receiving new tokens. The tokens can only be manipulated for the account that sends the transaction, therefore manipulation is further restricted. The exchange of a single good by user #5 is shown in Fig. 2.

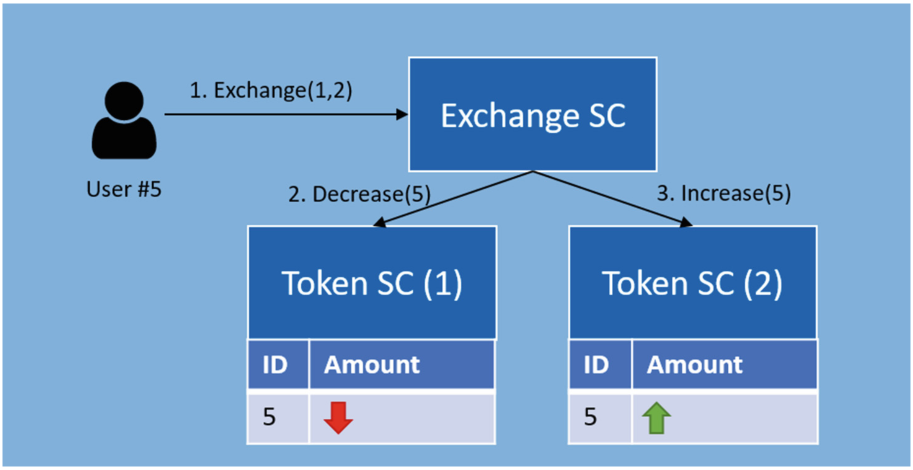

Fig. 2. Exchange of goods

3.3 Bootstrapping of the System

All participants of the supply chain have to use the proposed system or otherwise the system fails to provide all users the proposed functionality. If a supplier does not use the smart contract platform, the receiver of the goods cannot prove whether the good itself is from a valid source. The achieve a certain functionality, we have to ensure that a considerable amount of participants are using the system.

The idea for bootstrapping is as follows. From a game theoretical perspective, we have to encourage the users to participate in the Blockchain-based supply chain. Users which are just intermediaries do not gain an advantage of using the system, and they lose the ability to behave maliciously. It is questionable if the manufacturers of the base material do solely profit from introducing such a system if no other entities use the system. The only participants which heavily profit from the usage are large corporations which sell furniture or other goods made from sustainable wood. They have to prove to their customers the usage of economically friendly wood, otherwise their revenues would decrease. If the commercial customers are using the system, they can require that every merchant who provides them with wood has to use the system, which creates an incentive for all intermediaries to also use the system, as otherwise they would not be able to supply these companies. This also applies for other intermediaries which would start buying only from other suppliers which are able to actually provide certified wood in the system. If this happens, the easiest part is to convince the actual producers of the base material to introduce the system. They invest money in certifications and can increase their own revenue if they support a system that excludes their malicious competition from the market.

4 Discussion

4.1 Limitations

The introduced system exposes limitations due to the design of the Smart Contract architecture. We do not discuss limitations due to the nature of the used Blockchain technology and Smart Contract language such as transaction speed, anonymity, or susceptibility to errors. As technology advances, these limitations are likely to vanish.

Other limitations remain. The following list enables a brief overview of other possible strategic alignments of digital supply chains.

Loss of Information. A problem we introduced in Sect. 2 remains: The loss of information. As goods are recombined or merged, only a probabilistic assumption can be given about the origin of a single product. Furthermore, from a technical point of view we are not able to expand the platform in such way that it supports a provenance lookup. The introduction of meta-data is possible, but it remains unclear how the merging of meta-data from different sub-products would look like. As of our problem statement, this limitation is not relevant to our use case, as we are only interested in the consistent volume of goods managed by the system.

Exchange of Certified with Uncertified Products. Our system does not introduce digital twins, meaning that a digital good cannot be linked to a real-world good without doubt. As we only consider volumes, it would be possible for malicious entities to swap high quality (certified) wood with lower quality (uncertified) wood and sell it as certified. He would only benefit from that fact when a market exists for high quality wood outside of the supply chain where the entity is not required to send the tokens digitally. Again, our use case mainly focuses on prevention of volume manipulation. The damage incurred by swapping is low in comparison to volume manipulations.

Introduction of New Types of Products. An organizational problem could be the introduction of new products which require different amounts of other goods. First, the participants of the network have to agree to valid "exchange" rates: How much resources are required to create another product? Depending on the manufacturing process and the efficiency of the different manufacturers, these numbers can differ. This can lead to two problems: A manufacturer has to use more tokens than necessary on the Blockchain, basically “burning” tokens or it has to use less tokens than required, allowing the entity to introduce uncertified products into the supply chain. A way to mitigate the problem is that the manufacturer defines its conversion rates itself. In that case, other participants would have to validate whether these conversion rates are realistic or not. Generally, the participants have to be clear about their processes and the best way to mitigate risks is to develop sound exchange rates before implementing the system.

4.2 Applicability

We propose our solution for the use case of a timber-tracking supply chain. With limitations, one can apply the distributed application for other areas of supply chains.

Components for Electronic Devices. Electronic devices such as smart phones, notebooks or televisions consists of many base components which then again consist out of rare earths or other resources. Workers can get exploited in mining these goods, also the operators can exploit nature for their profit. With a system similar to our application, these drawbacks can be eliminated. The limitation would apply at that point in the supply chain as products are tracked on an individual level.

Ingredients of Food or Other Eatable Items. An additional supply chain system based on measurement of volumes is the food industry. By involving many stakeholders and intermediaries, the origin of base products such as wheat, corn as well as fish or meat can be used for malicious purposes. Some ingredients are intentionally mis-labeled, leading to a economical damage with potential health damages for consumers. For example, in 2013 horse meat was sold as beef which was unfit for human consumption [15]. With a proof, that meat originates from certified farms, one can complicate the manipulation.

5 Conclusion

In this paper, we present a solution for volume manipulation in large supply chains. The proposed exchange smart contract embedded in the system enables a transformation of base goods into other products according to predefined values, ensuring an overall sound maximum volume of base resources. Further advancements describe possible bootstrapping processes to introduce this digital solution in the industry. Future work can evaluate approaches to enable tracking of goods in supply chains on an individual level. Additional work has to be done to ensure a fully functional platform in case of non-participating entities.

References

1. Datta, S.P.A.: Emergence of digital twins. arXiv preprint arXiv:1610.06467 (2016)
2. Düdder, B., Ross, O.: Timber tracking: reducing complexity of due diligence by using blockchain technology (position paper). In: 2nd Workshop on Managed Complexity. CEUR-WS. org (2017)
3. Griggs, D., et al.: Policy: sustainable development goals for people and planet. Nature **495**(7441), 305 (2013)
4. Grunert, K.G.: Food quality and safety: consumer perception and demand. Eur. Rev. Agric. Econ. **32**(3), 369–391 (2005)
5. Hackius, N., Petersen, M.: Blockchain in logistics and supply chain: trick or treat? In: Proceedings of the Hamburg International Conference of Logistics (HICL), pp. 3–18. epubli (2017)
6. Hoare, A.: Tackling illegal logging and the related trade. Chatham House **2**, 21–47 (2015)
7. Hugos, M.H.: Essentials of Supply Chain Management. Wiley, Hoboken (2018)
8. Ireland, R.D., Webb, J.W.: A multi-theoretic perspective on trust and power in strategic supply chains. J. Oper. Manage. **25**(2), 482–497 (2007)
9. Korpela, K., Hallikas, J., Dahlberg, T.: Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
10. Lomas, N.: Everledger is using blockchain to combat fraud, starting with diamonds, https://techcrunch.com/2015/06/29/everledger (2015)
11. Miles, M.P., Covin, J.G.: Environmental marketing: a source of reputational, competitive, and financial advantage. J. Bus. Ethics **23**(3), 299–311 (2000)
12. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
13. NEPCon: FSC certification. https://www.nepcon.org/certification/fsc
14. News, U.: Un agricultural agency and european union step up efforts to combat illegal timber trade. URL: https://news.un.org/en/story/2016/05/529172-un-agricultural-agency-and-european-union-step-efforts-combat-illegal-timber
15. Premanandh, J.: Horse meat scandal-a wake-up call for regulatory authorities. Food Control **34**(2), 568–569 (2013)
16. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., Newton (2015)
17. Vlosky, R.P., Ozanne, L.K., Fontenot, R.J.: A conceptual model of us consumer willingness-to-pay for environmentally certified wood products. J. Consum. Mark. **16**(2), 122–140 (1999)
18. Vogelsteller, F., Buterin, V.: ERC-20 token standard, September 2017, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-tokenstandard.md
19. Wilding, R.: The supply chain complexity triangle: uncertainty generation in the supply chain. Int. J. Phys. Distrib. Logist. Manag. **28**(8), 599–616 (1998)
20. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper **151**, 1–32 (2014)