Anselm Busse, Jacob Eberhardt, Sebastian Frost, Dong-Ha Kim, Thore Weilbier, Lukas Renner, Matthias Roth, Stefan Tai

A Response to the United Nations CITES Blockchain Challenge: Incremental and Integrative PoA-based Permit Exchange

Accepted for 2019 IEEE International Conference on Blockchain and Cryptocurrency.

Busse, A., Eberhardt, J., Frost, S., Kim, D.-H., Weilbier, T., Renner, L., … Tai, S. (2019). A Response to the United Nations CITES Blockchain Challenge: Incremental and Integrative PoA-based Permit Exchange. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE. https://doi.org/10.1109/bloc.2019.8751373

A Response to the United Nations CITES Blockchain Challenge: Incremental and Integrative PoA-based Permit Exchange

Anselm Busse*
anselm.busse@tu-berlin.de

Jacob Eberhardt*
jacob.eberhardt@tu-berlin.de

Sebastian Frost*
frost@campus.tu-berlin.de

Dong-Ha Kim*
dong-ha.kim@campus.tu-berlin.de

Thore Weilbier*
thore.h.weilbier@campus.tu-berlin.de

Lukas Renner*
l.renner@campus.tu-berlin.de

Matthias Roth†
matthias.roth@adesso.ch

Stefan Tai*
tai@tu-berlin.de

*Technische Universität Berlin, Berlin, Germany
†adesso Schweiz AG, Zürich, Switzerland

***Abstract*—The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) negotiated and administered by the United Nations Environment Programme (UNEP) regulates the international trade of endangered species and derived products through a permit-based system. Currently, the permit process is paper-based and hence highly prone to manipulations and errors. Being aware of blockchains' potential, the CITES Secretariat defined a challenge to determine whether a blockchain-based system can address the aforementioned issues and serve as a secure, efficient, and affordable permit processing system.**

In this paper, we respond to the CITES Blockchain Challenge. First, we analyze the permit process and discuss how blockchain systems can improve that process in a way traditional systems cannot. Building on these results, we design a blockchain-based system that enables secure, manipulation- resistant permit validation, produces an immutable record of processed permits, and is in compliance with the CITES agreement. To evaluate this design, we developed a proof-of-concept implementation compatible with the paper-based permit process and deployed it to a Proof-of-Authority-based blockchain network. This allows incremental adoption and integration with the existing process, thereby increasing acceptance and addressing affordability. Finally, we describe how a blockchain- based system could disruptively improve the established permit process by enforcing quotas and tracking provenance.

***Index Terms*—blockchains, smart contracts, permits, provenance, supply-chain, CITES**

I. Introduction

The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) is an international agreement to ensure that trade of plants, animals, and products derived thereof does not threaten survival of the species [1]. CITES has currently been ratified by 183 parties [2] and regulates the trading of, currently, approximately 5,500 endangered animal and 29,500 plant species.

CITES requires the authorization of all imports, exports, re-exports, and introductions from the sea of covered species. These authorizations are managed and tracked in a permit process run between designated management authorities appointed by participating parties.

Today, the trading under CITES is completely paper-based with numerous drawbacks, e.g., fraud, counterfeiting, and long processing times. To improve on this process, eCITES, a set of software tools to support a digital version of the CITES permit process, was proposed several years ago. Expected benefits are mainly efficiency gains with regards to permit exchange and processing. No electronic permits, however, have been processed to date. eCITES is still in early adoption stage, with operational complexity and costs being main obstacles to a faster and broader adoption [3].

With the advent of blockchain technology in parallel to the development of eCITES and in addition to mere efficiency gains, improvements of the core process enabled by this novel class of systems seemed possible by enabling decentralized permit-validation and immutable recording of permit history. CITES, being aware of the problems of the paper-based process and the potential of blockchain technology, defined a challenge to determine whether a blockchain-based system can address the aforementioned issues and serve as a secure, efficient, and affordable permit processing system [4]. Hence, the research question addressed in this paper is directly defined by the CITES blockchain challenge:

> "Can Blockchain implement a system for secure, efficient and affordable exchange of CITES permits between authorized Parties and private sector stakeholders that is based on the existing, paper-based business processes?" [4]

978-1-7281-1328-9/19/$31.00 ©2019 IEEE

In this paper, we respond to this question. First, we analyze the paper-based permit process and discuss how blockchain systems can improve that process in a way traditional systems cannot. As a core contribution, we design a blockchain-based system that enables secure, manipulation-resistant permit validation and produces an immutable record of processed permits. This system is in compliance with the CITES agreement and integrates with the existing paper-based process to enable gradual onboarding of parties.

To evaluate this design and to show how it can be deployed in practice, we developed a proof-of-concept implementation and deployed it to a private blockchain network. Our implementation combines state-of-the-art smart contract engineering along with a carefully composed tool chain and cloud deployment. In this blockchain network, we use a *Proof-of-Authority (PoA)* mechanism that is a class off Byzantine fault-tolerant consensus algorithms. In a private setup, PoA can replace the highly compute intensive proof-of-work and is significantly more energy and resource efficient. In our architecture, CITES parties can become authorities who create new blocks and secure the network. Lightweight mobile clients ensure ease of adoption. Further, we demonstrate how this solution can meet worldwide CITES processing requirements in a cost-efficient manner.

Together, our design and implementation affirmatively answer the research question posed by the CITES blockchain challenge and introduce a secure, efficient, and affordable blockchain-based permit process in full compliance with the currently deployed paper-based process.

Finally, we outline how a blockchain-based system could change the permit process in a more disruptive way in the future. Securely enforcing trading quotas and tracking the provenance of species under CITES could be implemented if the requirement of full compatibility between the digital and the paper-based process were relaxed in the future.

The paper is structured as follows: Section II describes the CITES permit process in detail. The following section III discusses why the CITES process is a good candidate for a blockchain-backed solution. In section IV, we describe the architecture of our blockchain-based permit solution and our proof of concept implementation subsequently in section V. Section VI describes our test deployment. In section VII, we examine possible more disruptive changes to the permit-process enabled through blockchain technology. We discuss related work in section VIII and conclude our paper in section IX.

II. The CITES Permit Process

The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) is an international agreement between governments, which was signed in 1973 at the World Wildlife Conference. Besides other efforts, it mainly regulates the trading of, currently, approximately 5,500 endangered animal and 29,500 plant species. The convention has currently been taken into force by 183 parties [2]. The CITES is structured in a CITES Secretariat located in Geneva, Switzerland and national CITES management authorities designated and located in each participating country. The Secretariat is playing a coordination, advisory, and servicing role but does not enforce any rules or decisions. Binding decisions of, e.g., the trading quotas or the exclusion of trading of certain countries are made by the conference of the 183 parties.

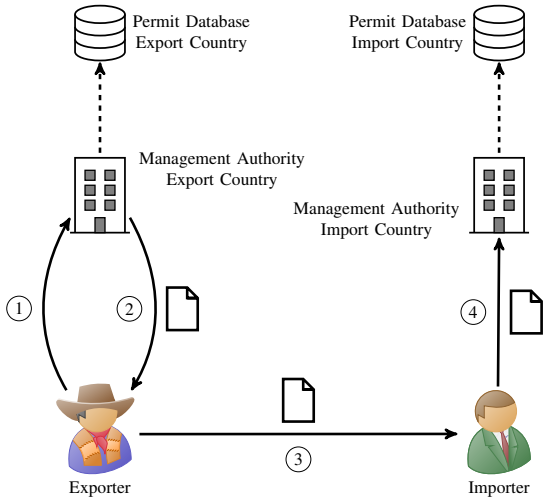


Fig. 1. The current paper based CITES permit process.

International trading of species covered by CITES is licensed by the national CITES management authorities. It is enforced through a paper-based permission process. This covers all imports, exports, re-exports, and introduction from the sea. The process is illustrated in fig. 1: When a legal entity, e.g., a company wants to export a specimen covered by CITES, it requests a permit at its local CITES management authority (step ① in fig. 1). If the CITES authority grants the export, it creates a paper permit that, besides the description of the specimen and the quantity, states the exporters' and importers' address (step ② in fig. 1). The paper permit accompanies the goods during their transport and is checked during the transport by authorities (step ③ in fig. 1). The paper permit is finally handed over to the local CITES management authority in the country of the receiver for bookkeeping purposes (step ④ in fig. 1). If the same specimen is supposed to be re-exported, a new permit from the local CITES management authority of the now exporting country is necessary. After the end of the year, the local CITES authorities send their import and export quantities to the CITES Secretariat. There, it is checked for quota violations and other irregularities. A violating party can be banned for trading under CITES through the conference of the parties.

The above process has several drawbacks and loopholes. First, a paper permit can be forged by creating a completely new one, by copying an existing one and reusing it for another export, or by manipulation of, e.g., quantities of species. This issue is mitigated by the CITES authorities by using physical copy protection for the paper permits. However, as with counterfeited bills, this process is not perfect and forged permits are still possible and used. Second, the process is time-

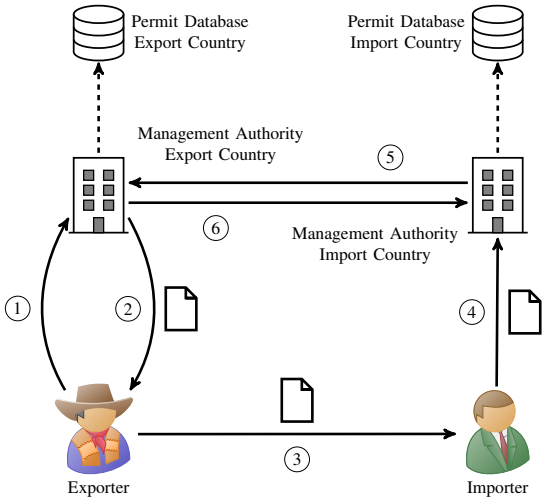


Fig. 2. The *eCITES* permit process. The paper permit can be validated through a digital channel between import and export management authority.

consuming and costly as the permit has to be printed on special paper by the local CITES authority to avoid counterfeiting and has to be send to the international forwarding agent. Depending on the local specifics of every country, this process can take up to several days. Third, it is costly to handle the paper permits both for the authorities and forward agents. Especially keeping them secure from forgery. And finally, the accounting towards the CITES Secretariat at the end of the year is time-consuming as the received paper permits have to be processed by the local CITES management authorities.

Because of the shortcomings of the paper-based permission process, *eCITES* was proposed to augment the process through an electronic data exchange (cf. [5]). It modifies the permit process as illustrated in fig. 2. Instead of verifying the legitimacy of the import based on the paper permit only, it is checked through an electronic request to the issuing authority (step ⑤ and ⑥ in fig. 2). Even though looking very mature from our perspective, the process is currently only deployed between Switzerland and France (cf. [6]) and until today, no permit was processed through this system. We suspect two reasons that slow down the adoption. First, because of the CITES structure, it is a peer to peer process. That makes it necessary that the servers of the issuing party are highly available. This might not state a problem for a highly developed country but might be an issue for poorly developed countries. And second, the deployment requires infrastructure that might also be hard to set up for less developed countries.

III. Blockchain Argument

Even though the research question for this paper given through CITES only asks whether blockchain technology can be used for the permit process, we want to discuss whether this is reasonable or not. Therefore, we will take into account the organizational structure and properties of CITES and selected non-functional requirements.

A. CITES Structure

Even though very powerful, blockchain technology does not fit every use-case. Below, we discuss the organizational properties of CITES that makes it a fitting use-case.

1) High Decentralization: The CITES organization by itself is highly decentralized. Every member operates completely independent throughout the year without the interference of other members or the CITES Secretariat. They decide whether they allow or deny a particular export and issue the corresponding paper permit. During the year, they are not monitored on how and to whom they issue permits for a particular reason. The only monitoring that gives the incentive to abide the rules is the gathering of all permits at the end of the year by the CITES Secretariat to do an analysis if the country did not exceed its export quota.

2) Limited Trust: Corruption is a widespread problem throughout the world [7]. As trading with endangered species can be highly lucrative and profitable, the CITES process can be the target of corruption on many levels. On the lowest level, individual or multiple employees could be bribed to issue fraudulent permits. On the highest level in highly corrupt countries, the government or parts of it could try to influence the local CITES authority or collude with other countries in order to manipulate the export process.

3) Transparency: The CITES process can benefit from transparency in two ways. First, transparency can mitigate the issues regarding corruption as discussed above. Independent third parties can audit the trading process and expose possible misuse. Furthermore, the possibility alone of an auditing by a third party at any time increases the risk of being detected misusing the system, therefore, lowering the incentive to do it in the first place.

Second, transparency can make the broader public aware of the import and export quantities and specimens of every country. If those are unacceptable, the public can influence politics in order to reduce or abandon the trade in certain areas. This would ultimately support the goal of CITES of ensuring survival of the species in question.

4) Protracted Decision Finding: With more than 180 parties involved in the negotiation of CITES, finding a consensus is a lengthy process and changes to the agreed upon consensus are also very difficult. This means as a consequence that the processes will not change often and dramatically. Therefore, an electronic system that supports the agreed upon processes does not have to be highly adaptable.

5) Heterogeneous Partners: Besides the degree of susceptibility to corruption, the participating countries are very heterogeneous regarding other aspects resulting in different capabilities and agendas. Some countries are rather rich and developed and have both a developed infrastructure and the capability to run a sophisticated setup, whereas other less developed countries lack both. For some countries, flexibility and delay regarding the issuing of permits are more crucial than the absolute number of exports, while in other countries it is the other way around. Some countries have more imports than exports, some are balanced and some have more exports

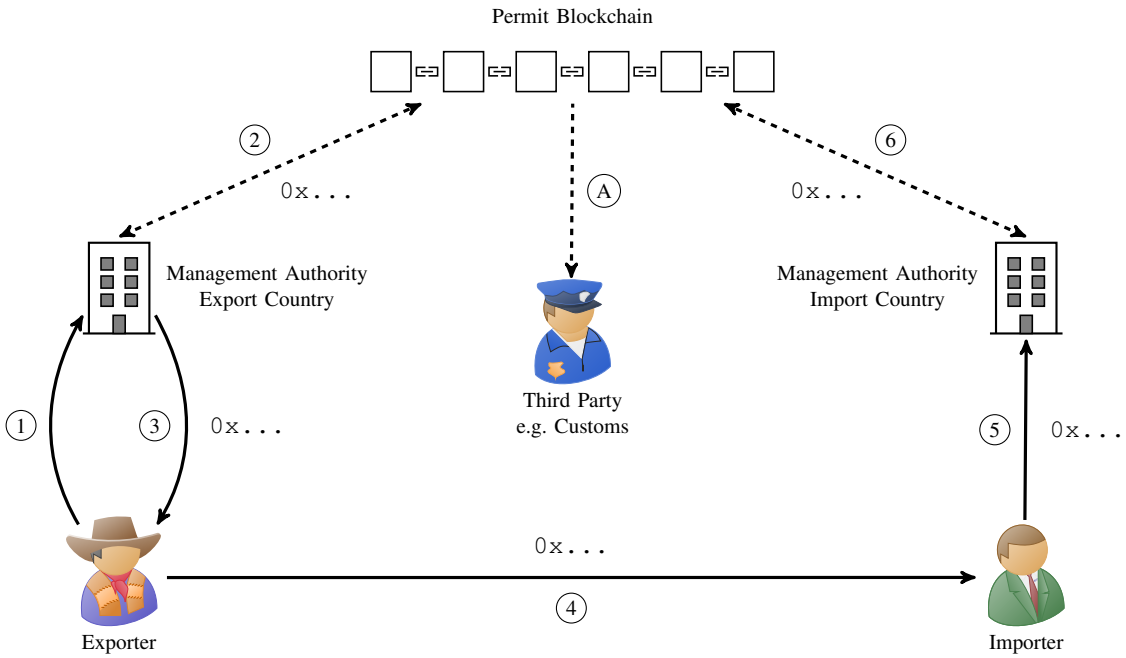


Fig. 3. The blockchain-based permit process. The paper permit process is augmented through a blockchain that stores all permits and their status. Process actors receive a permit hash instead of a paper permit. Additional actors can access and validate the permit information.

than imports. Some countries have a very high number of trades, others have a very limited number. All these differences result in different requirements for the trading system and different incentives and capabilities to adopt a new digital system.

B. Non-Functional Considerations

The CITES challenge as quoted in the introduction already implies some non-functional challenges that have to be taken into account:

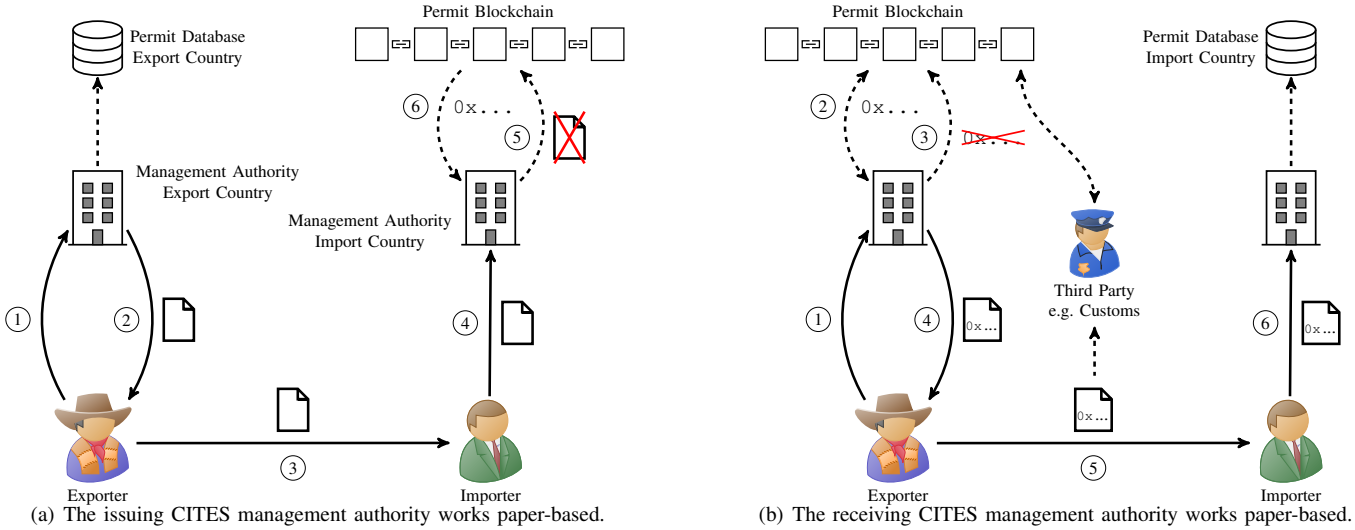
1) Costs: As discussed above, the countries that have signed the CITES agreement are very diverse. We suspect that for a significant number of countries the costs of joining an electronic CITES system are a crucial factor, either absolute or relative to the provided benefit. For example, some countries lack the appropriate Internet infrastructure that would be necessary to run the system or their local CITES authority is missing the manpower and/or expertise to set up the system and does not have the financial resources to have the system run by an external contractor. For other countries, the costs of establishing and running the necessary server infrastructure would exceed the benefit as the trade with endangered species does not have a notable share on the economy.

2) Complexity: Having a distributed system with more than 180 independent participants and no central authority can be very challenging for traditional setups. This includes the setup itself, as every member has to be connected to each other resulting in an n:n setup. Furthermore, the data has to be held consistent between all participants, which can result in a significant effort. It can be expected that smaller countries are unable to cope with these issues.

IV. Blockchain-based Permit Process

Based on the assessment in section III, we built a proof of concept for a blockchain- based CITES permit process. In order to achieve acceptance by the stakeholders, we decided to implement the blockchain solution in a minimal invasive manner. Our approach maintains the current process as it is agreed upon by all parties and widely accepted, while tackling shortcomings of the paper-based process.

The blockchain-based permit process is depicted in fig. 3. It starts the same way as the paper-based permit process with an exporter that requests a permit from the local CITES management authority (step ① in fig. 3). Instead of issuing a paper permit, the management authority creates a digital permit that is stored on the blockchain and identified through a unique KECCAK-256 hash (step ② in fig. 3). It can be transmitted to the exporter in an arbitrary way, e.g., through email or paper that does not have to be secured in any way. (step ③ in fig. 3). This identifier accompanies the exported good in the same way as the paper permit does today (step ④ in fig. 3). Again, this could happen via paper, but also through electronic means like a document on a smartphone or tablet. Given the permit data and its identifier every party is able to verify the integrity of that permit. Analogue to the current paper-based process, the permit identifier is handed over to the importing CITES management authority (step ⑤ in fig. 3) and it processes the permit on the blockchain and invalidates the permit so it cannot be used again (step ⑥ in fig. 3). Based on the decentralized manner of the blockchain, it is also possible to allow a third party like, e.g., customs to verify the validity of the permit in order to stop illegal trade as early as possible (step Ⓐ in fig. 3).



(a) The issuing CITES management authority works paper-based.

(b) The receiving CITES management authority works paper-based.

Fig. 4. The two corner cases of integrating the blockchain-based permit process into the existing paper-based permit process. Note that the blockchain instance is shared with other not depicted countries that use the blockchain process.

Two corner cases exist in this architecture, when deployed in the current setup:

1) The exporting country does not support blockchain-based permits, but the importing country does (fig. 4(a))
2) The importing country does not support blockchain-based permits, but the exporting country does (fig. 4(b))

In the first case, a paper permit will be submitted to the CITES management authority of the importing country. Therefore, the first four steps are the same as in fig. 1. The authority creates a blockchain-based permit with the same information, but already invalidated as the permit was already used for the import (step ⑤ in fig. 4(a)). In order to minimize any chance for misuse, it destroys the paper permit permanently. Further, processing of the permit for, e.g., statistics happens using the blockchain-based copy (step ⑥ in fig. 4(a)).

In the second case, the CITES authority of the exporting country will first create a blockchain- based permit after the exporter requests it (step ② in fig. 4(b)). However, it immediately invalidates the digital permit as it will not be used but is still present on the blockchain for analytics (step ③ in fig. 4(b)). In the next step, it will issue a classical paper permit fitting to the current process, however, the paper permit can reference the blockchain permit (step ④ in fig. 4(b)). This would allow third parties to at least verify the permit partially and could prevent certain types of fraud like e.g., changing the species or quantities in the permit. The rest of the process is the same as in fig. 1.

V. Implementation

The main components of the implementation are shown in fig. 5. It consists of the *blockchain backend*, the *smart contracts* and *User Interfaces* for interacting with the system. A description of each component follows below. The implementation is available at GitHub[1].

[1]https://github.com/cites-on-blocks/cites-on-blocks_dapp

A. Blockchain Backend

Regarding the blockchain technology to build upon, we decided to use *Ethereum* as it has the biggest development community, resources, and tools at the time of writing of this paper. It allowed us to use a private *Proof-of-Authority (PoA)* setup to achieve a higher throughput of transactions, while leaving the opportunity to migrate to public blockchain for further research and if desired by CITES later on. For the proof of concept, we opted for the PoA setup assuming that

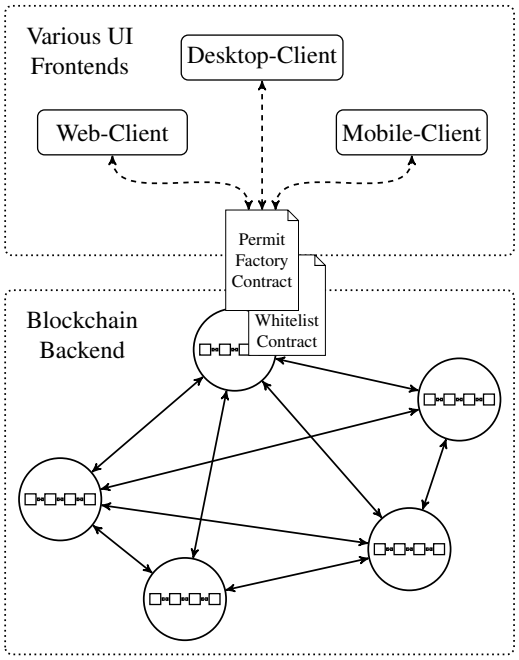
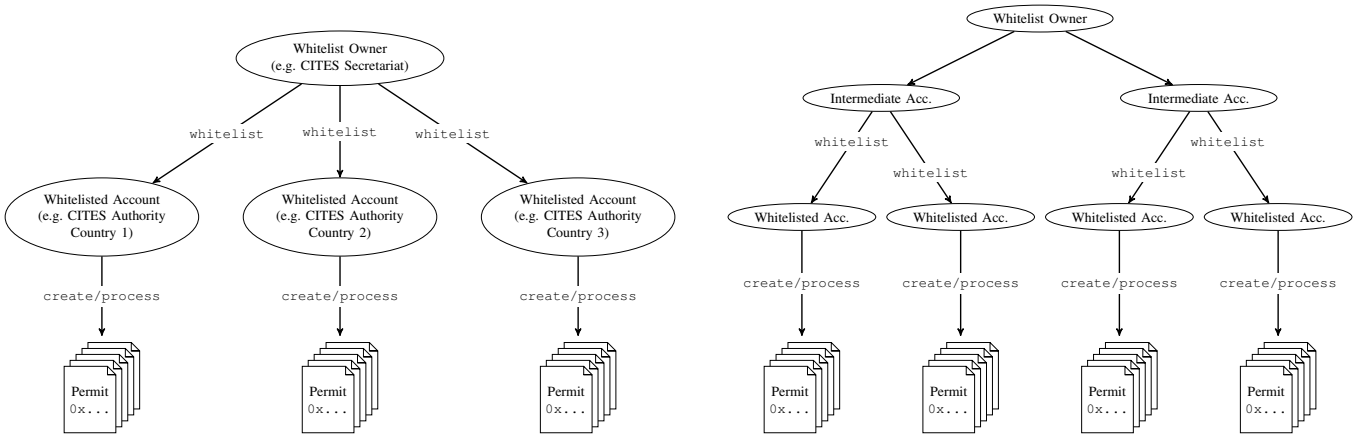


Fig. 5. The system architecture for the blockchain-based permit process. Different clients and clients implementations can connect to the same blockchain network through the contract API.



(a) Permission scheme of the proof of concept implementation.

(b) Possible extension to a multi-level permission scheme.

Fig. 6. Permission schemes for permit creation and processing.

each CITES authority might host an authority node themselves to secure the blockchain in a truly decentralized nature. Therefore, an equal distribution between the participants will be needed to avoid scenarios where a minor subset of parties can force a fork of the chain in their interest. As this technical requirement also touches the political structure of CITES, we cannot propose a final setup. As the administration costs of running a node are non-negligible, we assumed that several countries will cooperate to run one node and therefore the number of total nodes will be small.

B. Smart Contracts

The business logic of the blockchain-based CITES permit process is implemented in two contracts written in *Solidity* and uses the well audited *OpenZeppelin* library[2]: the `Whitelist` and the contract. The first is used to manage access rights whereas the second contains permit related functionalities. Note that the actual implementation of the contracts is available through the project's GitHub repository mentioned above.

1) `Whitelist` Contract: To ensure that only authorized accounts can create permits, we implemented a whitelisting scheme in the `Whitelist` contract for permit creation. Through the `Ownable` contract of the *OpenZeppelin* library, only the owner of this contract is allowed to call functions that mutate the data on the whitelist. In practice, the accounts can be mapped, e.g., to specific countries and CITES employees. The owner of the `Whitelist` contract, in practice, will be the CITES Secretariat. The included features of the contract are:

- Add and remove management authorities for countries to and from the whitelist
- Add and remove users of the management authorities to and from appropriate countries

Although write access is restricted to the owner of the contract, read access is granted to everyone. As further contribution to the logic, it provides methods to check permissions and responsibilities for users, which like to interact with the `PermitFactory` contract.

2) `PermitFactory` Contract: The business logic of the digital permit issuance itself is implemented in the `PermitFactory` contract. Authorized accounts, respectively users on the above described whitelist, are able to create digital permits for their assigned country they are responsible for. It is to mention that they are only allowed to issue a permit in which their assigned country is the exporting country. Same goes for finalizing permits when importing. In case of a country issuing a paper-based permit, only authorized users of the importing country are able to digitalize this permit subsequently. Therefore, blockchain-based permits that origin from paper-based permits differ on who creates and signs them.

Currently, the contract also serves as a storage for all permits and their related data. This makes calling the function to create permits very expensive in terms of transaction costs. In a private PoA setup, this fact is negligible but can become significant if considering migrating to a public setup. Nevertheless, the storage size of the chain will grow indescribably fast.

The current relation between the whitelisting and permit creation is summarized in fig. 6(a). Note that for the purpose of this proof of concept, we implemented only one layer for the whitelisting process. In practice, it might be necessary, to implement multiple layers: The CITES Secretariat will whitelist single accounts for each country that can subsequently whitelist further accounts allowed to create permits. This would result in a tree structure as depicted in fig. 6(b) where the CITES Secretariat is the root, the leafs are allowed to create permits and intermediate accounts are different levels of the management hierarchy in local CITES management authorities.

[2]https://github.com/OpenZeppelin/openzeppelin-solidity

C. User Interfaces

In order to facilitate the interaction with the *Smart Contracts*, we implemented different user interfaces. We opted for multiple clients to show the independence of the user interface from the underlying blockchain implementation. This shows that in a production deployment single CITES members could develop their own client tailored to their needs.

1) Web-User-Interface: In order to demonstrate the entire functionality of the blockchain-based implementation, we built a web-based user interface. It is based on the *Javascript* framework *React* and relies on *MetaMask* for handling account and key management. It supports the basic features of the `Whitelist` contract as well as the one of the `PermitFactory` contract. Furthermore, it contains a section for analytics where the collected data are processed. Several diagrams visualize information, e.g., how much specimens of what kind a country has ex-/imported over which period of time. All information can be filtered and categorized. It demonstrates the general possibilities of the data analytics enabled by the blockchain approach as compared to the paper-based approach.

The web-interface also includes an export service that allows the export of the permit to an XML file or to generate a PDF that could be used in the process of generating a permit for an export to a non-blockchain-enabled country.

2) Native Clients: In order to demonstrate the flexibility, three native clients were developed. Their functionality was determined by a separation of concerns. One desktop application that only interfaces with the `Whitelist` contract demonstrates a possible specialized client for the CITES Secretariat. Two Clients with CITES authorities in mind that only interface with the `PermitFactory` contract were developed; one for desktop and one for mobile use. The desktop applications were developed for *macOS*, while the mobile application was developed for *iOS*. All three are using the *Swift* programming language. The *web3swift* [3] library is used to communicate with the *Ethereum* nodes. The account keys are stored locally in standard *Ethereum JSON keystore* files protected through a password stored in the operating systems' keychain.

An URL scheme was introduced for simpler sharing and processing of a permit:

```
citesbc://permit/[permit-hash]
```

This allows to easily include a blockchain permit in an email and the encoding through a QR code. A video demonstrating the native client is available online.[4]

VI. Deployment

We tested our implementation in two different deployments and did an initial scalability test. As discussed in section V-A, we opted for a PoA setup.

A. Container-Based Deployment

The first deployment used the *Microsoft Azure* platform with a *Standard D2s v3* instance (2 vCPUs, 8 GB Memory). We instantiated three instances of the stable Parity container[5] as authority nodes in a *PoA Ethereum* network. The network was configured to use *Aura* as PoA with a round time of one second. We instantiated three more instances of the same container as none-authority members. The Web-Interface is run through *Nginx* on the same machine. The Docker-Setup allowed initial testing and scalability studies (see below).

B. Virtual Machine Deployment

The second setup used virtual machines in our local *OpenStack* setup consisting of three *Nova* compute notes. We created three virtual machines — one running on each compute node — running *Gentoo Linux* and the *Parity* client. Again, we formed a PoA network with a round time of one second. Furthermore, we deployed the web user interface to one of the machines as well. We allowed access to one of the parity nodes from the outside of the *OpenStack* setup trough an *Nginx* proxy secured by a simple password authentication and transport layer security through a *Let's Encrypt*[6] certification. A valid certificate was necessary in order to run the native applications as it is required by macOS and iOS.

C. Scalability

A complete and extensive scalability study of our proof of concept is beyond the scope of this paper. However, we conducted a small test with three local authority nodes using the Aura consensus algorithm with a step duration of one second. We were able to reach up to 18 transactions while keeping the uncle rate below 1%. This would result in up to more than $5 \cdot 10^8$ transaction per year. Even doing a pessimistic estimate with all permits created during eight hour work days, five days a week would result in more than 10^8 permits per year. Considering that the current number of issued permits per year is well below two million [1], it is safe to say that the system will most likely be able to handle the permit issuing in the foreseeable future.

VII. Re-inventing Blockchain-based Permit Processing

The paper-based permit process described in section II is part of the internationally negotiated CITES agreement. Hence, to remain compatible with this agreement, the system design introduced in section IV is strictly compliant with that process. However, a blockchain-based system could provide additional desirable properties to the permit process if the process could be altered. In this section, we outline these properties that could be enabled by permit process disruption.

[3] https://github.com/BANKEX/web3swift

[4] http://dx.doi.org/10.14279/depositonce-8250

[5] https://hub.docker.com/r/parity/parity/

[6] https://letsencrypt.org

A. Product Provenance

As discussed above, the trading with endangered species is lucrative and prone to corruption. A fully blockchain-based permit process could ensure that all products traded under the CITES agreement have an unforgeable digital history and hence implement a provenance system for endangered plants, animals, and derived products. By allowing verification of a product's origin, this system could provide valuable information to customers who seek to consume responsibly. However, a fully featured provenance system may also be opposed by parties who do not wish to disclose their supply-chain information in a blockchain network.

Although this approach could significantly improve the effectiveness of CITES regarding its goal to protect endangered species, we assessed that it would be politically hard to enforce. Some CITES parties would likely oppose a highly transparent system that allows the tracking of every specimen and related supply-chain information to not lose their competitive advantage or put their revenue streams at risk. A solution to this dilemma could be a system with optional provenance tracking on an opt-in basis that allows participants who are willing to reveal the information to submit it to the blockchain. This would result in a digital history only for some specific products, but those products could possibly be sold to a higher price than equivalent products without history, thus, creating a potential incentive to parties to willingly provide the provenance information publicly.

B. Reporting and Automatic Sanctioning

In the current CITES process, the trading volume is only evaluated once a year individually for each country based on the permits issued and received by that country. Hence, quota violations are only detected during end of the year checks by the CITES Secretariat. Violators can be banned from trading under CITES if agreed on by the parties at the CITES conference.

With a fully blockchain-based process, reporting can happen more frequently as the data is widely available. Furthermore, the data can be aggregated from multiple countries and checked against each other, which makes it very hard to hide quota violations.

In an even further evolved system, violations could automatically be detected and even sanctioned through the use of cryptocurrencies. Furthermore, it would also be possible to automatically enforce trading quotas within smart contracts. Issuance of permits that would violate quotas could automatically be prevented.

C. Organizational Governance

The CITES parties participate in the organization's governance process, mainly through voting during the yearly CITES conference. This leads to a slow decision making process and high coordination overhead. In the future, a blockchain-based system could include a digital governance platform that would allow the CITES parties to coordinate and make their decisions in a more transparent and efficient way. For example, a smart contract could dynamically adjust each party's quorum rules and related sanctions after an on-chain vote of CITES parties.

VIII. Related Work

Our response to the CITES challenge was presented, along with a demonstration, during a meeting in the CITES Secretariat on November 28th, 2018 in Geneva, Switzerland. According to the CITES officials, no other responses to the CITES challenge do yet exist. Furthermore, there is little research relating to blockchain-backed permit processes. Khaqqi, Sikorski, Hadinoto, *et al.* [8] discuss emission permit trading building on the *MultiChain* Platform. However, their main focus is on selling and buying of permits and not on the issues regarding fraud.

Blockchain-systems that track the provenance of physical goods are already described in literature. Hannam [9] for example describes the tracking of the provenance of tuna, Loebbecke, Lueneborg, and Niederle [10] discuss the one of diamonds and Thiruchelvam, Mughisha, Shahpasand, *et al.* [11] the one of coffee. However, they do not tackle the issue of limiting and controlling the trade of the goods between countries. Several more systems tackling provenance exist and are described in literature [12]–[14]. Another application of blockchain technology is logistics and supply chain management. Several research papers discuss this approach [15]–[18]. Still, permit processing and trade control are not addressed in this prior work.

IX. Conclusion and Future Work

In conclusion, our work shows that the CITES process cannot only be implemented using blockchain technology but can also be improved. It becomes more transparent and accessible to the different stakeholders while maintaining the incidence of the individual countries regarding issues permits. We have shown that the transition can happen in a minimal invasive manner country by country without migrating all participants at once. Furthermore, we have discussed more invasive features that are enabled through blockchain technology and might augment the process later on.

In the future, we plan to maintain and deepen our dialog with the CITES Secretariat and possibly extend it to selected CITES management authorities. We plan to discuss the prototype and decisions made during the construction. As the challenge is limited regarding information concerning specific requirements, we hope to be able to improve the prototype further to the needs of CITES in order to make it a starting point for a real system deployment that handles real permits.

For the proof of concept, we have only conducted a limited set of measurements regarding scalability in order to determine the general suitability of the approach regarding the workload specific to CITES. As a next step, we plan to do more extensive benchmarks. We plan to distribute the location of the authority nodes over the world as it would probably be the case in a production environment. We also plan to take other measurements besides throughput into account like delay and robustness.

References

[1] The CITES Secretariat. (2018). What is CITES? [Online]. Available: https://www.cites.org/eng/disc/what.php (visited on Dec. 5, 2018).

[2] ——, (2018). List of parties to the convention, [Online]. Available: https://cites.org/eng/disc/parties/index.php (visited on Dec. 3, 2018).

[3] ——, (2017). Automation of CITES permit procedures and electronic information exchange for improved control of international trade in endangered species (eCITES), [Online]. Available: https://cites.org/sites/default/files/eng/prog/e/eCITES_policy_briefing.pdf (visited on Dec. 4, 2018).

[4] ——, (Nov. 2017). The CITES blockchain challenge, Can blockchain prevent the use of fraudulent CITES certificates and permits? [Online]. Available: https://cites.org/sites/default/files/eng/com/sc/69/inf/E-SC69-Inf-33.pdf.

[5] M. Pikart. (2017). The eCITES implementation framework, A practitioners guide to implement electronic CITES permits, [Online]. Available: https://cites.org/sites/default/files/20180219eCITESImplementationFramework.pdf (visited on Dec. 3, 2018).

[6] The CITES Secretariat. (2018). eCITES, [Online]. Available: https://cites.org/eng/prog/eCITES (visited on Dec. 3, 2018).

[7] Transparency International, *Global Corruption Report 2004*. Pluto Press, Jul. 2004, ISBN: 0-7453-2231-X.

[8] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Applied Energy*, vol. 209, pp. 8–19, Jan. 2018, ISSN: 0306-2619. DOI: 10.1016/j.apenergy.2017.10.070.

[9] K. Hannam. (Sep. 2016). This emerging tech company has put asia's tuna on the blockchain, Forbes, [Online]. Available: https://www.forbes.com/sites/keshiahannam/2016/09/30/this-emerging-tech-company-has-put-asias-tuna-on-the-blockchain/ (visited on Dec. 4, 2018).

[10] C. Loebbecke, L. Lueneborg, and D. Niederle, "Blockchain technology impacting the role of trust in transactions: Reflections in the case of trading diamonds," in *Proceedings of the 26th European Conference on Information Systems*, ser. ECIS2018, Jun. 2018. [Online]. Available: http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledgerAssociation (visited on Dec. 4, 2018).

[11] V. Thiruchelvam, A. S. Mughisha, M. Shahpasand, and M. Bamiah, "Blockchain-based technology in the coffee supply chain trade: Case of burundi coffee," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, no. 3-2, pp. 121–125, Sep. 2018, ISSN: 2180-1843.

[12] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proceedings of the 17th International Symposium on Cluster, Cloud and Grid Computing*, ser. CCGrid '17, Madrid, Spain: IEEE Press, 2017, pp. 468–477, ISBN: 978-1-5090-6610-0. DOI: 10.1109/CCGRID.2017.8.

[13] Project Provenance Ltd., "Blockchain: The solution for transparency in product supply chains," Project Provenance Ltd., White Paper, Nov. 2015. [Online]. Available: https://www.provenance.org/whitepaper (visited on Dec. 4, 2018).

[14] modum.io AG, "Data integrity for supply chain operations, powered by blockchain technology," modum.io AG, White Paper, 2017. [Online]. Available: https://modum.io/sites/default/files/documents/2018-05/modum-whitepaper-v.-1.0.pdf (visited on Dec. 4, 2018).

[15] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62 018–62 028, Oct. 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2875782.

[16] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," in *Proceedings of the 2017 Symposium on Integrated Network and Service Management*, May 2017, pp. 772–777. DOI: 10.23919/INM.2017.7987376.

[17] F. Tian, "An agri-food supply chain traceability system for china based on RFID & blockchain technology," in *Proceedings of the 13th International Conference on Service Systems and Service Management*, ser. ICaSSSM 2016, Jun. 2016. DOI: 10.1109/ICSSSM.2016.7538424.

[18] S. Abeyratne and R. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 05, pp. 1–10, 09 Sep. 2016. DOI: 10.15623/ijret.2016.0509001.