Neisse, Ricardo; Hernandez-Ramos, Jose Luis; Matheu-Garcia, Sara Nieves; Baldini, Gianmarco; Skarmeta, Antonio; Siris, Vasilios; Lagutin, Dmitrij; Nikander, Pekka

An Interledger Blockchain Platform for cross-border Management of Cybersecurity Information

Published in:
IEEE Internet Computing

DOI:
10.1109/MIC.2020.3002423

Published: 01/05/2020

Document Version
Publisher's PDF, also known as Version of record

An Interledger Blockchain Platform for Cross-Border Management of Cybersecurity Information

Ricardo Neisse
European Commission, Joint Research Centre

José L. Hernández-Ramos
European Commission, Joint Research Centre

Sara N. Matheu-García
University of Murcia

Gianmarco Baldini
European Commission, Joint Research Centre

Antonio Skarmeta
University of Murcia

Vasilios Siris
Athens University of Economics and Business

Dmitrij Lagutin
Aalto University

Pekka Nikander
Aalto University

***Abstract*—Cybersecurity certification is a core notion to support the mitigation of cybersecurity risks of Information and Communication Technologies (ICT). At the European Union (EU) level, the Cybersecurity Act establishes a common cybersecurity certification framework supporting the coexistence of different certification schemes across Member States. However, its realization needs to be sustained by technical approaches to enable ICT stakeholders from different sectors or countries to exchange cybersecurity information and evaluate the up-to-date security level of an ICT system throughout their lifecycle. Toward this end, we propose a blockchain-based platform using a novel interledger design, where ledgers associated with ICT artifacts, cybersecurity certificates, and vulnerabilities are interconnected. The main purpose is to leverage the advantages of blockchain in terms of distributed trust, transparency, and accountability, while at the same time coping with scalability, performance, and interoperability requirements. We analyze the impact of our platform in the current EU legislation and provide insights for its deployment.**

Digital Object Identifier 10.1109/MIC.2020.3002423
Date of publication 17 June 2020; date of current version 21 July 2020.

Published by the IEEE Computer Society

In an increasingly technology-dependent world, providing a harmonized view of cybersecurity is crucial for the deployment of trustworthy ICT infrastructures. For this reason, cybersecurity certification has become a cornerstone concept to enhance the acceptance of the digital age.[1] The advent of technologies such as 5G or Internet of Things (IoT)[2] promises to realize the vision of a hyperconnected society, in which humans and devices compose complex interconnected systems leading to a strong cybersecurity interdependence. To achieve a trusted interdependence, the cybersecurity certification process cannot be carried out for a single device in isolation, but considering its communications and interactions within a system and external components. This represents a significant challenge when a system is made up of different components, which are certified according to schemes from different sectors/countries. Furthermore, this vision of hyperconnectivity implies that a vulnerability affecting a system in a country or domain may have a cascading impact on systems in other domains/countries. Therefore, an integrated cross-border and cross-sector sharing approach is essential to make cybersecurity certification information available in an accurate and coherent way.

At the European Union (EU) level, the Cybersecurity Act[3] represents an ambitious effort to provide a common European Cybersecurity Certification Framework. This framework will provide coordinated governance to improve the current situation where multiple certification schemes are used in different member states (MS) to certify ICT artifacts (the term "artifact" is used to represent an ICT product, service, or process in the rest of the article) and are not mutually recognized. The Cybersecurity Act complements the Network and Information Security (NIS) Directive,[4] which is focused on the cooperation and exchange of security information among MS. Both initiatives identify several challenges that are addressed in this article. First, there is a need to manage the security updates and patches during an artifact's lifecycle, since they will affect to its cybersecurity (re-)certifications.[5] The analysis of such data could help us to determine relationships between vulnerabilities, as well as to anticipate the emergence of new attacks. Second, manufacturers/providers must be identifiable and accountable for possible deficiencies (either intentional or unintentional) with respect to self-declared compliance of an ICT artifact to specific cybersecurity requirements. Furthermore, there is a lack of a vulnerability sharing platform for certain ICT artifacts (e.g., in the context of IoT[5]) to enable a responsible vulnerability disclosure[6] allowing manufacturers/providers to prepare patches and notify users in a timely and reliable way.

Based on these challenges, we propose a blockchain platform to support the management of cybersecurity certification and vulnerability information in the EU. The use of Distributed Ledger Technologies (DLTs) (like blockchains[7]) is a promising approach to enable a trustworthy and transparent platform for sharing cybersecurity information among providers/manufacturers and consumers at different MS or domains that do not share a common trusted third party.[8] Moreover, considering the possible large number of ICT artifacts, as well as the potential changes in their security level (e.g., due to a new cybersecurity certificate), a large number of blockchain transactions needs to be considered, raising scalability and performance issues. To cope with these aspects, we propose to partition our platform in multiple interconnected (block)chains deployed across MS following a hierarchical approach based on *interledger* mechanisms.[9] In our proposed platform, an EU Cybersecurity Chain is maintained at EU level by a consortium of all MS to support the coordination and interconnection of different chains at MS level to manage manufacturer/provider information and the ICT artifact lifecyle (e.g., updates, and patches), cybersecurity certification information,[10] and responsible vulnerability disclosure. Unlike a simple network of national servers, the advantage of our blockchain-based approach is that it enables collaboration, cooperation, and ensures transparency and immutability of the cybersecurity information to be shared among stakeholders across sectors/countries. Furthermore, our platform eases the tracking of versions related to cybersecurity certificates and software/firmware updates that is crucial to anticipate potential risks in a certain deployment. While a network of national servers could be implemented to provide the same

services (which in practice could be similar to a blockchain platform), the following section describes additional advantages of our proposed platform. It should be noted that this article is an extension of our previous publication,[11] which proposed a preliminary design for managing certification information without considering interledger concepts.

This article is organized as follows. Section "Cybersecurity Certification: Regulatory Requirements" analyzes the relevant EU regulations in the context of cybersecurity certification and information sharing. Based on this, Section "Blockchain-Based DLTs and Interledger Approaches" provides an overview of the interledger approach and the mechanisms that are used in our platform. Section "Platform Architecture" describes our platform by considering the different stakeholders, and the deployment of interledger mechanisms. Then, Section "Use Case Scenario" describes a use case scenario, where our platform is used for sharing cybersecurity certification information, and to support the responsible vulnerability disclosure. Section "Evaluation Results" provides some evaluation results about our proposal, and Section "Conclusion" concludes the article.

CYBERSECURITY CERTIFICATION: REGULATORY REQUIREMENTS

The Cybersecurity Act and the NIS Directive identify a set of requirements and needs to support the deployment of an European Cybersecurity certification ecosystem. The following sections describe such requirements and provide insights on how our proposed platform will address them.

Sharing of Cybersecurity Information

In a hyperconnected world, cyberattacks have a borderless nature, and their impact could affect critical infrastructures in different institutions or countries. Therefore, providing access to the corresponding cybersecurity information is crucial to foster the realization of a more homogeneous perspective on cybersecurity at the EU level. Both the Cybersecurity Act and NIS Directive promote strategic cooperation among MS to support and facilitate sharing of information. The information to be considered could include data about recently detected attacks or vulnerabilities found on specific ICT artifacts. Based on this, our proposed platform acts as a cross-border information sharing tool where smart contracts[11] are used to support and regulate the sharing process in a harmonized and transparent way among the stakeholders.

Coexistence of Multiple Certification Schemes

The intended cybersecurity certification framework will support different certification schemes across the EU, since each MS currently does not use the same scheme. To mitigate this issue, the Cybersecurity Act is aimed to improve the harmonization of the cybersecurity certification processes across MS. Indeed, it is expected that different schemes from certain countries or covering the requirements of specific components will be still in force. In this heterogeneous context, a cross-border and cross-sector approach is required to identify the relationship among different schemes, so that ICT artifacts certified under a certain scheme can be still recognized in other countries or sectors. Indeed, in most of the cases, a certificate issued by a national authority is not recognized in other MS. Therefore, companies may be obliged to certify their ICT artifacts using different cybersecurity certification schemes for each country where they have a market deployment, which is not cost effective and goes against the main principles of the European Digital Single Market. An additional aspect is that a certain artifact could be (in turn) composed by different components that could be certified under different schemes. In this direction, our platform could help to identify the relationship among the components of a composed ICT artifact in a transparent and trusted way through the use of interledger mechanisms.

Cybersecurity Certification Throughout an ICT Artifact's Lifecycle

A major requirement for any cybersecurity certification scheme is to provide certification support throughout the lifecycle of an ICT artifact that could be affected by the discovery of new potential vulnerabilities/cyberattacks, or

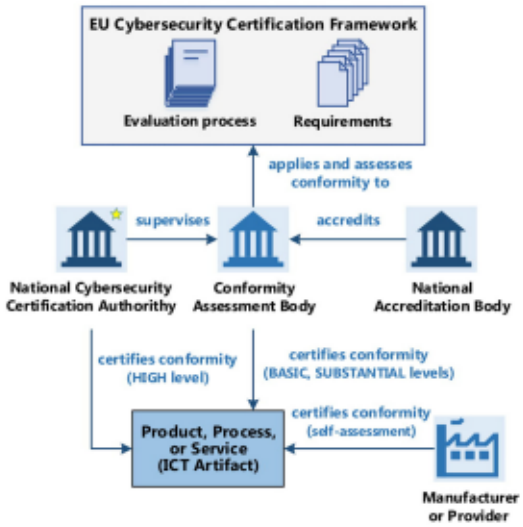

Figure 1. Overview of the proposed EU Cybersecurity Certification Framework.

the installation of a security update/patch. In other words, there is the need to provide assurance continuity for all the lifecycle of ICT artifacts. Beyond the requirements for the process itself, a key issue is how to make this information available, taking into account the scale of the number of ICT artifacts. Therefore, there is a need to adopt an integrated approach to transparently reflect the security level of an artifact. We believe that the proposed interledger approach takes advantage of the inherent nature of blockchain in terms of immutability and transparency to reflect the cybersecurity level throughout the artifact's lifecycle.

Support for Self-Assessment Procedures

According to the Cybersecurity Act, a cybersecurity certificate is issued depending on a certain *assurance level*, which represents a basis for confidence that an ICT artifact meets certain security requirements. The assurance level describes the rigor and depth of an evaluation, and could be "basic," "substantial," and "high." Figure 1 depicts the relevant stakeholders according to the proposed EU certification framework. Conformity Assessment Bodies, which are accredited by a National Accreditation Body and supervised by a National Cybersecurity Certification Authority, apply and assess the conformity of ICT artifacts considering a common evaluation process and requirements defined in a scheme. For "basic" and "substantial" assurance levels, the Conformity Assessment Bodies issue the cybersecurity certificate. However, for a "high" assurance level, a National Cybersecurity Certification Authority (or a Conformity Assessment Body under specific circumstances) is responsible for this. In the case of the level "basic," a certification scheme may allow for conformity self-assessment under the sole responsibility of the artifact's manufacturer/provider, which makes the corresponding information available to the national authorities. An advantage of this process is to avoid the whole certification process, which could be an expensive procedure. However, self-assessment could lead to significant issues if the process is not carried out in a transparent way by legitimate manufacturers and providers. In this context, our decentralized platform will be used to share self-assessment information to make it visible to the corresponding authorities and stakeholders.

Increasing Cybersecurity Awareness

Another purpose of the Cybersecurity Act is to promote a high level of cybersecurity awareness among citizens, organizations, and businesses. In this direction, the deployment of a pan-European platform for cross-border cybersecurity information management would contribute to increase such awareness. On the one hand, the intended blockchain platform will allow users to have access to the cybersecurity information concerning their ICT artifacts. This information could be also complemented with guidelines and recommendations about the use of a certain component, as well as the vulnerabilities associated with it. On the other hand, such a platform could be also employed by citizens and companies to share cybersecurity information and recommendations. Indeed, the use of a blockchain-based platform could help to track the state of a newly disclosed vulnerability, in order to promote the enforcement of *responsible vulnerability disclosure* procedures.[6]

BLOCKCHAIN-BASED DLTS AND INTERLEDGER APPROACHES

A blockchain is a type of Distributed Ledger Technologies (DLTs) that offers a decentralized solution for collaboration and interoperability. One of the main features of DLTs is the

immutability of data: ledgers are append-only databases where existing data cannot be modified and only new data can be added. Another major feature is a *distributed consensus mechanism*, which controls what and how data are added to the ledger. Furthermore, DLTs also *replicate* data to participating nodes thus improving availability. Because of these three properties, DLTs mitigate the risk of a single point of failure and offer resilience against different cybersecurity attacks. It is relatively easy to determine if any of the participating nodes in the DLT is misbehaving and, even if an attacker manages to control the majority of the DLT's resources, (s) he cannot modify the existing data, only control the addition of new data. Indeed, the main practical innovation of DLTs is the enabling of distributed trust.

DLTs allow various entities, which may not fully trust each other, to collaborate in a verifiable and transparent manner, so that misbehavior can be easily identified or even prevented by design using *smart contracts*. DLTs can be implemented with different levels of openness. They can be fully *open* (permissionless), which means that anyone can join the DLT and propose transactions, such as Bitcoin.[12] However, DLTs can also be permissioned, either in a *semiopen* way, where read access is open to everyone but write access is restricted, or in a *closed* way, where both read and write access are restricted to a consortium of organizations (e.g., Hyperledger Fabric[13]).

There exists a large number of DLTs providing different tradeoffs in terms of latency, throughput, consensus algorithm, and functionality, to be considered in different applications. For example, a DLT can focus on cryptocurrency payments, recording of IoT events, or access authorization. In complex systems, it is therefore often not feasible to use a single DLT for everything, hence the *interledger* approach[9] is required in many situations to allow different DLTs to exchange data with each other. Indeed, the main goal of interledger mechanisms is to enable the transfer of value and/or information among blockchains while transactions are cryptographically linked to ensure some dependence relation among them. Some examples of interledger mechanisms include the use of hash-lock and time-lock mechanisms in transactions or smart contracts running on the different blockchains.

Hash-locks are used to cryptographically link transactions on different ledgers by including the condition that a secret is submitted whose hash is equal to a specific value. If the secret is submitted to one of the ledgers, then the secret can be obtained by all entities with read access to that ledger. Hence, an entity can obtain the secret from the ledger where it was revealed, and submit it on the other ledger with the same hash-lock. Such an approach ensures that, if the secret is revealed on one ledger, then the transaction on that ledger and all other linked transactions (i.e., the transactions with the same hash-lock on the other ledgers) are executed. Moreover, time-locks can be used to add transactions whose execution depends on time. Specifically, time-locks can be used to allow some transactions to be executed only after some time has elapsed. For blockchains, time is related to the block creation time and it can be expressed as an absolute value (i.e., transaction execution after/before a specific block is mined) or relative (i.e., transaction execution when a specific number of blocks have been mined after the current block).

In addition to the aforementioned mechanisms, linking of data on different ledgers can be achieved by taking hashes of data recorded on one ledger and recording these hashes on another ledger. Such an approach can be used, for instance, to store data on permissioned blockchains having a lower degree of decentralization and periodically storing hashes of that data on a more decentralized ledger. This can be achieved using a *sidechain* approach, where a system of nodes (functionaries) overlook and verify transactions that move assets between a main/parent chain to its sidechains.

The following section presents our proposed platform showing how the interledger concepts were used to support cross-border management of cybersecurity information. In this article, we adopt the term *Chain* to refer to a semiopen permissioned blockchain-based DLT, even though we are not referring to any specific technical implementation choice.

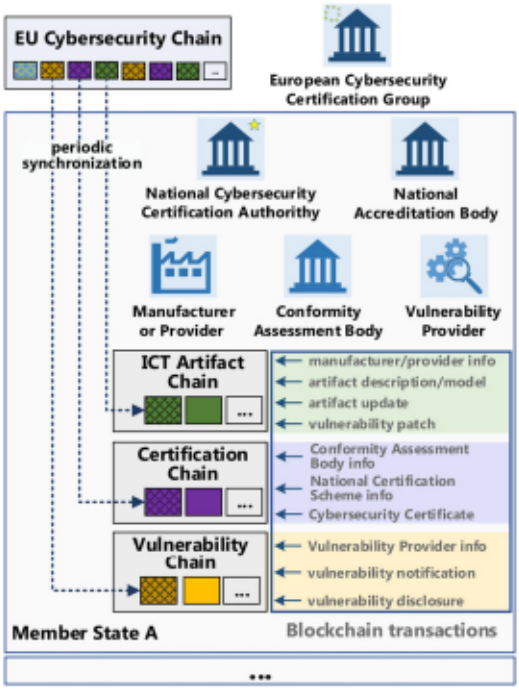

Figure 2. Interledger architecture for managing cybersecurity information.

PLATFORM ARCHITECTURE

Based on the roles defined in the Cybersecurity Act (see Figure 1), an overview of our proposed platform is shown in Figure 2. Our platform consists of one *EU Cybersecurity Chain*, managed at European level and three chains deployed for each MS at national level, namely: *ICT Artifact Chain*, *Certification Chain*, and *Vulnerability Chain*. The chains in our platform are not used to store large amounts of information; any data file requiring substantial amount of storage is stored off-chain in a database, and only a reference (including hashes to verify the integrity) are added to the blockchain transactions.

The EU Cybersecurity Chain relies on interledger mechanism to interconnect the ledgers deployed at national level where the genesis block of each chain and (periodically) a synchronization block are published in the EU Cybersecurity Chain. According to the interledger terminology,[9] national ledgers could be considered as *sidechains* that are interconnected to a *main* chain represented by the EU Cybersecurity Chain. The time threshold for synchronization is a tradeoff between the time period (between synchronizations), where the national chains may be potentially modified, and the performance and scalability overhead. The analysis of these parameters is out of the scope of this article. The EU Cybersecurity chain also stores the identity information of EU and national authorities, and the information related to the EU cybersecurity certification framework that is shared across MS (e.g., the adopted cybersecurity certification scheme or process).

The chains proposed in our platform are permissioned with a clearly defined consortium of nodes authorized to write transactions and to validate blocks, which is also managed through the EU Cybersecurity Chain. The management of the consortium identities is intended to be performed using a smart contract, where the EU and national authority identities are registered following our previous work.[11] At EU level, the *European Cybersecurity Certification Group* (defined by the Cybersecurity Act) groups representatives of national authorities, and it is responsible for the identity management procedures and for validating transactions. It should be noted that the EU Cybersecurity Chain represents a trust anchor in our platform, in order to reach a tradeoff between the benefits provided by such as decentralized approach, and the need to consider main EU institutions to coordinate/manage the sharing ecosystem for cybersecurity information. According to the roles defined by the Cybersecurity Act, the mentioned EU Cybersecurity Certification Group, together ENISA and the European Commission could be in charge of the EU Cybersecurity Chain distributing authority powers to the national authorities. Indeed, our approach is intended to keep track of the cybersecurity information history of ICT artifacts. The rules on how the such information is reported are defined by the Cybersecurity Act and the NIS Directive.

The ICT Artifact Chain is used to manage manufacturer/provider information and identities, models and description of the ICT artifacts, firmware updates, and vulnerability patches. The Certification Chain supports the management of accredited national Conformity Assessment Body identities, information about national certification schemes and their mappings to the EU cybersecurity certification framework, and cybersecurity certificates issued by national

assessment bodies. Moreover, the purpose of the Vulnerability Chain is to provide traceability of vulnerabilities discovered by accredited vulnerability providers (e.g., cybersecurity researchers, companies), which can also have their identities managed through this chain, in order to support responsible disclosure. For example, a vulnerability provider can announce that a vulnerability was found in a specific product, including a reference to the product in the ICT Artifact Chain, without revealing publicly the vulnerability. After a certain amount of time, and allowing the product manufacturer to release a specific patch, the vulnerability provider could publicly disclose the vulnerability.

For the interconnection of the blockchains proposed in Figure 2, we envision the usage of hash-lock and time-lock mechanisms. Used together, they ensure atomicity in the execution of transactions on different ledgers, i.e., either all transactions that are linked through these mechanisms are executed, or none are executed. In the proposed architecture, hash-lock mechanisms are used to link vulnerability notification events to a specific artifact and smart contract functions, which are triggered by vulnerability events, such as an automated compensation in another chain (e.g., Bitcoin payments) when a vulnerability is discovered under a bug bounty program. Furthermore, hashes of the data recorded on the national ledgers can be recorded on the EU Cybersecurity Chain.

As a consensus mechanism, we propose all chains to adopt Proof-of-Authority (PoA), where the representatives of the European Cybersecurity Certification Group act as validators. In a practical implementation, for example, using Hyperledger Fabric, these entities would be responsible for endorsing the transactions. Indeed, in Hyperledger, the consensus consists of three phases: endorsement, ordering, and validation. In case of our architecture, the specific validation/endorsement policy (e.g., two or more MS) will depend on governance aspects, agreements, and the technical blockchain solution adopted. Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus are not suitable for these scenarios since PoW is typically used in public blockchains where the validators are not clearly identifiable, and PoS is also not applicable because there is not explicit values at stake like in a blockchain dedicated to digital assets (e.g., cryptocurrency). PoA is more suitable in this case because of the reputation of the nodes validating the transactions, which are the respective representatives from the MS. The decision and assignment of the authorities to the representatives are coordinated at EU level by the European Cybersecurity Certification Group. The three chains operated at national level should also adopt a PoA consensus, where the validators will be respectively the Manufacturers/Providers, Conformity Assessment Bodies, and Vulnerability Providers. The registration and accreditation of these entities at the MS level is coordinated by the National Cybersecurity Certification Authority and National Accreditation Body. It should be noted that the validators in these chains will not be responsible for validating the transaction content, but only the correctness of the transaction structure and execution aspects.

USE CASE SCENARIO

Based on the proposed platform, Figure 3 shows the interactions required to manage the cybersecurity information during the lifecycle of an ICT artifact (see Section "Cybersecurity Certification Throughout an ICT Artifacts Lifecycle"). The management is done using smart contracts deployed in the three chains used to handle information about ICT artifacts, cybersecurity certificates, and vulnerability information. The access to the information in the chains and submission of transactions is performed using a blockchain client, which is shown in Figure 3 in the ICT User Domain.

When a new ICT artifact is manufactured, the corresponding manufacturer/provider uses the *Artifact Registry* smart contract in the *ICT Artifact Chain* to register references to information about such artifact. The information itself is stored in the *ICT Artifacts Database*, and can be used by the Conformity Assessment Body (or the National Cybersecurity Certification Authority) to carry out the certification process. For example, this information could include results of testing processes carried out during the manufacturing process, as well as a model-based representation and description of the ICT artifact itself.[10] Furthermore, as described in the

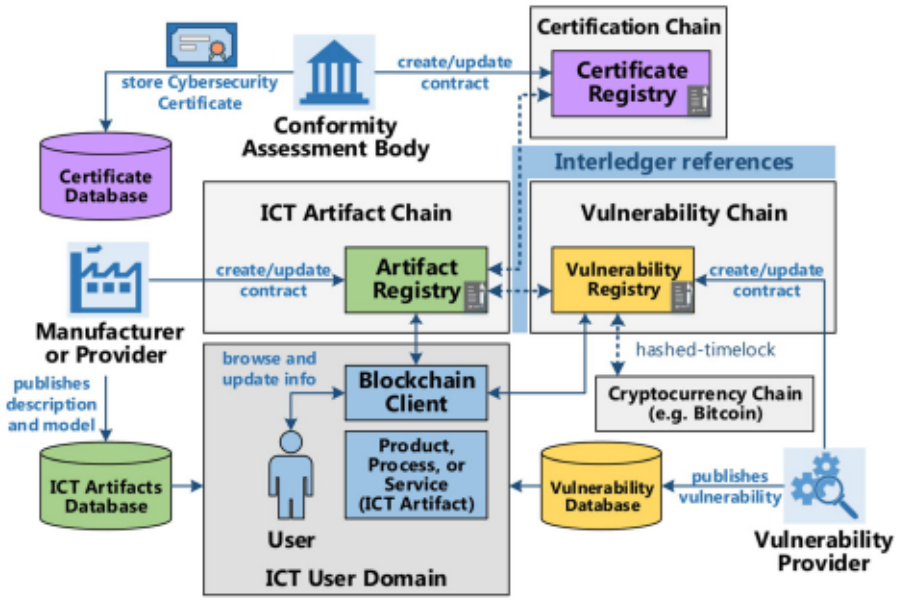

Figure 3. Scenario to manage cybersecurity information of an ICT artifact.

Section "Increasing Cybersecurity Awareness," the Cybersecurity Act mentions the need to provide additional information about an ICT artifact, including security guidelines and recommendations to help end users with configuration, installation, deployment, operation, and maintenance. For example, in the case of specific-purpose artifacts (i.e., IoT devices), the recent Manufacturer Usage Description (MUD) standard[14] could be used to foster a secure and automated deployment of a certain IoT device, as proposed by Neisse *et al.*[11] An additional aspect is related to the software libraries that are part of the artifact. This information could help us to identify specific components that are affected by a cybersecurity issue or vulnerability.

In Figure 3, the Conformity Assessment Body or the National Cybersecurity Certification Authority depending on the assurance level (see Section "Support for Self-Assessment Procedures") publishes references to the certification information using the *Certificate Registry* smart contract, including the required elements defined in a certain European cybersecurity certification scheme. These elements include the evaluation criteria and methods used for the certification, as well as the validity period and rules for monitoring the compliance of the certificate. The information itself is stored in the *Certificate Database*. The specific level of assurance and certification constraints can be handled by the logic implemented in the Certificate Registry smart contract.

The published Certificate may make reference to information provided by manufacturer/provider in the ICT Artifact Chain. In addition, it could make reference to chains in other MSs to reflect the dependencies among different artifacts composing a certain system (see Section "Coexistence of Multiple Certification Schemes"). For example, a certain ICT product could be composed by different artifacts that were manufactured in different MSs, and potentially certified by different certification schemes. Therefore, each artifact's certificate could be stored in a different chain, which could be referenced by the chain where the product certificate is stored. Beyond tracking the security level of a single artifact, this approach would allow us to maintain the traceability of the artifacts' certificates (and their relationships) composing a certain ICT artifact.

During the artifact's lifecycle, new vulnerabilities might be detected, so that a new cybersecurity certification process is required. Indeed, the Cybersecurity Act mentions the need to provide references to repositories where vulnerabilities associated with a certain ICT artifact can be found. As already mentioned, our platform uses a *Vulnerability Chain* for each MS that references

the ICT Artifact chain to represent the artifacts (and their associated software versions) that are affected by a certain vulnerability. For this purpose, the corresponding bodies (e.g., specialized companies) acting as a *Vulnerability Provider*, are in charge of reporting vulnerabilities by using the *Vulnerability Registry* smart contract. In addition to the data related to the vulnerability itself (e.g., the identifier of the affected software), the execution of this smart contract could trigger other actions in a different chain because of the interledger approach (e.g., labeling a certain software version as *vulnerable* in the ICT Artifact Chain). As shown in Figure 3, a transaction in a Cryptocurrency Chain (e.g., Bitcoin) could also be triggered if the Vulnerability Provider is entitled for a compensation as a result of having found a specific vulnerability.

Beyond fostering the alignment of different certification schemes to reduce current fragmentation (see Section "Coexistence of Multiple Certification Schemes"), there is also a need of a common format to represent the information about cybersecurity vulnerabilities, and associated attacks or incidents. In this direction, the use of an expressive and standardized approach could help to foster an interoperable cybersecurity information sharing approach across sectors and countries (see Section "Sharing of Cybersecurity Information"). To cope with this aspect, the use of approaches such as the Structured Threat Information Expression (STIX)[15] could help to complement our interledger platform with an additional degree of interoperability.

EVALUATION RESULTS

A performance evaluation of the proposed framework was conducted using the SimBlock tool[16] for the vulnerability chain. Even if SimBlock is originally designed for PoW, the tool was tailored to model PoA by adjusting the configuration parameters with a very low mining difficulty.

The original network and simulation configuration of SimBlock were modified to represent the European context. In particular, the block generation interval was set to 10 min, the number of regions configured to the 27 EU Member States, and the number of nodes was set to the current number of Computer Security Incident Response Teams (CSIRTs) for each region, with 348 blockchain nodes.[17]

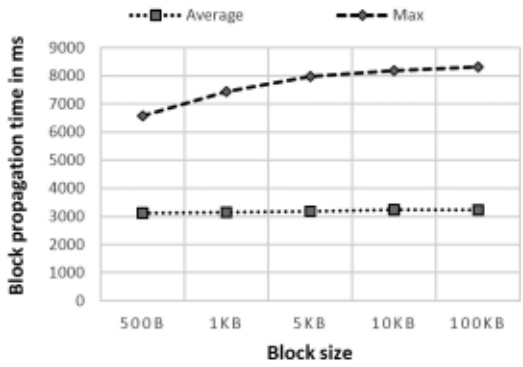

Figure 4. Average and maximum block propagation time for the vulnerability chain for different values of the block size in bytes.

Two metrics were used to evaluate the performance of the vulnerability chain: the average and the maximum block propagation time across all the nodes for different block sizes. These metrics are used by Aoki *et al.*,[16] where it is shown that the block propagation time is directly linked to the overall throughput of the blockchain and the number of transactions per block.

Figure 4 shows the simulation results, where it can be seen that the block propagation time of nearly 3 s is still reasonable for an EU wide network. However, the proposal to limit the block size has its merits because with the increase of the block size, the maximum block propagation time increases significantly, even if the average time does not grow substantially. Considering our scenario, where the blockchain transactions will only contain references to an off-chain database, and the need of processing at least one transaction per minute for the vulnerability chain (in the first trimester of 2020, 1 transaction per minute was the average number for the National Vulnerability Database[18]), the simulation results confirm the feasibility of our blockchain platform proposal.

Due to space restrictions, we only present the evaluation of the vulnerability chain. The other chains proposed in our platform will have a similar behavior, and the vulnerability chain is the one with the higher expected transaction throughput rate. Therefore, the evaluation results can be generalized to prove the feasibility of the other chains.

CONCLUSION

The realization of an EU cybersecurity certification framework requires the adoption of suitable technological approaches to support a transparent and interoperable sharing of cybersecurity information. Toward this end, this article presented a blockchain-based platform to address some of the main requirements derived from current EU cybersecurity legislation by using interledger mechanisms, in which chains from different countries are interconnected. This approach allows different blockchain implementations at country level, while scalability and performance issues derived from single-ledger deployments are mitigated. Our proposal is intended to enable a trusted EU cybersecurity information sharing and coordination approach, where ICT stakeholders located in different MSs can have strong assurance guarantees about the rules for data sharing, encoded in the smart contracts, and in the data itself. While our proposal is the first attempt to efficiently manage the cybersecurity information sharing among stakeholders, the deployment of such platform represents our ongoing work in this area to evaluate technical and governance aspects of a possible deployment of our platform at EU level, in order to complement our initial simulation results.

REFERENCES

1. J. Voas and P. A. Laplante, "IoT's certification quagmire," *Computer*, vol. 51, no. 4, pp. 86–89, 2018.
2. M. R. Palattella *et al.*, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.
3. European Parliament, "European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the council on ENISA, the 'EU Cybersecurity Agency'," 2019.
4. European Union, "Directive (EU) 2016/1148 of the european parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union, OJ l 194, 19.7.2016, pp. 130." 2016.
5. S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a cybersecurity certification framework for the internet of things," *IEEE Secur. Privacy*, vol. 17, no. 3, pp. 66–76, May–Jun. 2019.
6. H. Cavusoglu, H. Cavusoglu, and S. Raghunathan, "Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge," *IEEE Trans. Softw. Eng.*, vol. 33, no. 3, pp. 171–185, Mar. 2007.
7. R. Maull, P. Godsiff, C. Mulligan, A. Brown, and B. Kewell, "Distributed ledger technology: Applications and implications," *Strategic Change*, vol. 26, no. 5, pp. 481–489, 2017.
8. R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, Art. no. 14.
9. V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger approaches," *IEEE Access*, vol. 7, pp. 89948–89966, 2019.
10. S. N. Matheu-García, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices," *Comput. Standards Interfaces*, vol. 62, pp. 64–83, 2019.
11. R. Neisse, J. L. Hernndez-Ramos, S. N. Matheu, G. Baldini, and A. Skarmeta, "Toward a blockchain-based platform to manage cybersecurity certification of IoT devices," in *Proc. IEEE Conf. Standards Commun. Netw.*, 2019, pp. 1–6.
12. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf
13. E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 30:1–30:15. [Online]. Available: http://doi.acm.org/10.1145/3190508.3190538
14. E. Lear, D. Romascanu, and R. Droms, "Manufacturer usage description specification (RFC 8520)," 2019. [Online]. Avaialble: https://tools.ietf.org/html/rfc8520
15. S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (stix)," *Mitre Corporation*, vol. 11, pp. 1–22, 2012.
16. Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, "Simblock: A blockchain network simulator," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2019, pp. 325–329.

17. ENISA, "The European CSIRT inventory," 2020. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory
18. National Institute of Standards and Technology, National Vulnerability Database, "Official common platform enumeration (CPE) dictionary statistics," 2020.

Ricardo Neisse has been a Scientific Project Officer with the Joint Research Centre, European Commission, Italy, in 2013. His research interests include cybersecurity engineering for mobile devices, cloud computing, blockchain platforms, Internet of Things, and enterprise systems. He received the Ph.D. degree in computer science from the University of Twente, The Netherlands, in 2012. Contact him at ricardo.neisse@ec.europa.eu.

José L. Hernández-Ramos is a Scientific Project Officer with the European Commission, Joint Research Centre. His research interests include the application of security and privacy mechanisms in the Internet of Things and transport systems scenarios, including blockchain and machine learning. He received the Ph.D. degree in computer science from the University of Murcia, Spain. He is the corresponding author of this article. Contact him at jose-luis.hernandez-ramos@ec.europa.eu.

Sara N. Matheu-García is currently working toward the Ph.D. degree from the University of Murcia, Spain. Her main research interests include the security certification for the Internet of Things. She received the B.S. degree in mathematics and the B.S. and M.S. degrees in computer science from the University of Murcia, Spain, in 2015 and 2016, respectively. Contact her at saranieves.matheu@um.es.

Gianmarco Baldini is currently a Scientific Project Manager with the Joint Research Centre, European Commission, since 2007. His research interests include Internet of Things, automotive technologies, wireless communication, and cybersecurity. He received the Laurea degree in electronic engineering from the University of Rome in 1993 and the Ph.D. degree in computer science in 2019. Contact him at gianmarco.baldini@ec.europa.eu.

Antonio Skarmeta is a Full Professor with the University of Murcia, Department of Information and Communications Engineering. His research interests include the integration of security services, identity, the Internet of Things, and smart cities. He has published more than 200 international papers and been a member of several program committees. He received the Ph.D. degree in computer science from the University of Murcia. Contact him at skarmeta@um.es.

Vasilios Siris is an Associate Professor with the Department of Informatics, Athens University of Economics and Business since 2009. His research interests include trusted communication in the Internet of Things (IoT), the application of blockchain and distributed ledger technology to the IoT, resource management and traffic control in wired and wireless networks, and architecture of future mobile and pervasive communication systems. He received the Diploma degree in physics from the National and Kapodistrian University of Athens in 1990, the M.S. degree in computer science from Northeastern University, Boston, USA, in 1992 and the Ph.D. degree in computer science from the University of Crete in 1998. Contact him at vsiris@aueb.gr.

Dmitrij Lagutin is currently the Coordinator and a Research Fellow in the EU Horizon 2020 SOFIE Project at Aalto University, Finland. He received the M.Sc. (Tech.) degree from the Helsinki University of Technology, Finland, in 2005, and the D.Sc. (Tech.) degree from Aalto University, Espoo, Finland, in 2010. His research interests include network security and privacy, self-sovereign identifiers, Internet of Things, blockchains, and future network technologies. Contact him at dmitrij.lagutin@aalto.fi.

Pekka Nikander has been a Professor of Industrial Internet with Aalto University, Finland, since 2017. He received the M.Sc. and Ph.D. degrees (Hons.) in computer science from Helsinki University Technology [(HUT), a predecessor of Aalto University], Finland, in 1992 and 1999, respectively. His research interests include the effect of the antirival properties of data and information to the structure of the economy. Contact him at pekka.nikander@aalto.fi.