International Journal of Information Security manuscript No.
(will be inserted by the editor)

INCHAIN: A Cyber Insurance Architecture with Smart Contracts and Self-Sovereign Identity on Top of Blockchain

Aristeidis Farao[1,2] · Georgios Paparis[1] · Sakshyam Panda[3] · Emmanouil Panaousis[3] · Apostolis Zarras[1,4] · Christos Xenakis[1,5]

Received: date / Accepted: date

Abstract Despite the rapid growth of the cyber insurance market in recent years, insurance companies in this area face several challenges, such as a lack of data, a shortage of automated tasks, increased fraudulent claims from legal policyholders, attackers masquerading as legal policyholders, and insurance companies becoming targets of cybersecurity attacks due to the abundance of data they store. On top of that, there is a lack of *Know Your Customer* procedures. To address these challenges, in this article, we present `INCHAIN`, an innovative architecture that utilizes Blockchain technology to provide data transparency and traceability. The backbone of the architecture is complemented by Smart Contracts, which automate cyber insurance processes, and Self-Sovereign Identity for robust identification. The effectiveness of `INCHAIN`'s architecture is compared with the literature against the challenges the cyber insurance industry faces. In a nutshell, our approach presents a significant advancement in the field of cyber insurance, as it effectively combats the issue of fraudulent claims and ensures proper customer identification and authentication. Overall, this research demonstrates a novel and effective solution to the complex problem of managing cyber insurance, providing a solid foundation for future developments in the field.

Keywords Cyber Insurance · Blockchain · Smart Contracts · Self-Sovereign Identity

✉ Aristeidis Farao <arisfarao@unipi.gr>
[1] Department of Digital Systems, University of Piraeus, Piraeus, Greece
[2] European Doctoral School, European Security and Defence College, Brussels, Belgium
[3] School of Computing and Mathematical Sciences, University of Greenwich, London, U.K.
[4] Foundation for Research and Technology – Hellas, Greece
[5] InQbit Innovations SRL., Romania

1 Introduction

The increasing shift towards the digital realm raises concerns about cybersecurity attacks, which can lead to substantial financial losses for corporations, amounting to millions or even hundreds of millions of dollars. However, the consequences of these attacks go beyond finances, posing risks to critical infrastructure, social cohesion, and mental health. Therefore, prioritizing effective cybersecurity measures is crucial to mitigate such risks. Recently, large-scale cybersecurity attacks rank third on the list of global threats [1]. Cyber insurance is the primary method for transferring insured financial risks and losses associated to networks and computers caused by cybersecurity incidents to a third party [2,3]. As a product, cyber insurance can aid Policyholders (PHs), encompassing both organizations and individuals, in mitigating the risks associated with cybersecurity threats. Nonetheless, the market for cyber insurance is currently at a pivotal moment, with significant implications for both Insurance Companies (ICs) and PHs.

ICs, on the one hand, are having trouble making a profit due to the growing number of claims and increasing expenses. First and foremost, this relates to the cyber insurance *Fraudulent Claims* and *Identity Theft* challenges. While the former occurs when dishonest PHs submit many claims for the same cybersecurity incident with several ICs, the latter happens when attackers masquerade as eligible PHs to submit false claims and steal the identity of others. Moreover, ICs have only a few years' worth of data to operate without having access to reliable data on their PHs' assets and security measures [4]. That rises from the *Lack of Data* (i.e., ICs do not have access to accurate data regarding PHs' assets, revenue amount, type of processed data, security controls, and frequency of cybersecurity

incidents) and *Lack of Know Your Customer* (i.e., ICs lack methods to gather PHs' accurate data and monitor their behavior) challenges. In addition, ICs become a natural target for cyber attacks as they possess substantial amounts of confidential PH data. That is directly related to the *Loss of Sensitive Data* challenge.

On the other hand, PHs have raised concerns not only from existing ICs but also from prominent ones. According to SOPHOS' 2022 report, 47% of the respondents noted that current policies are more complicated, which is attributed to the challenge of *Information Asymmetry* [5]. This occurs when there is an imbalance between two negotiating parties in their knowledge of relevant factors and details. Additionally, 37% of the respondents claimed that cyber insurance procedures take an extended period, which is linked to the *Lack of Automated Tasks* challenge. This happens because cyber insurance processes are often performed manually and are outdated, making them time-consuming.

The problems and challenges mentioned earlier have been encountered in numerous cybersecurity attacks. In 2017, Merck was hit by the NotPetya malware, resulting in a loss of more than $1.4B. Merck had $1.75B in property insurance and believed it would cover the costs caused by NotPetya. However, their IC rejected the claim because NotPetya was considered an act of war, and the insurance policy did not cover it [6, 7]. This indicates a misunderstanding regarding the coverage provided by the purchased insurance. Furthermore, LLOYD'S report presented the Shen attack scenario [8]. It is a hypothetical cyber attack on ports across the Asia Pacific, targeting the maritime supply chain, infecting 15 ports, and resulting in estimated losses of $110B. The report demonstrates that the global economy is unprepared for such an attack, with 92% of the total economic costs being uninsured.

Based on the above statements and established facts, our research aims to address the following questions:

RQ1: *Which are the main insurability challenges?*

RQ2: *Which are the primary stakeholders and processes of cyber insurance, and how do they interact to accomplish the goal of cyber insurance?*

RQ3: *How does the literature address existing cyber insurance challenges with Blockchain and Smart Contracts?*

In general, a thriving cyber insurance market should benefit all parties involved. Consequently, as the market for cyber insurance becomes increasingly complex, it becomes imperative to revise and adapt cyber insurance products to meet evolving demands and ensure that all stakeholders reap maximum benefits [9]. Rather than treating cyber insurance as a mere commodity in a soft market, it should be viewed as a means of protecting the balance sheet. In this respect, cyber insurance should be regarded as the last resort to mitigate losses in the event of a catastrophic cybersecurity incident.

In this article, we summarize the challenges in cyber insurance and introduce our innovative architecture, `INCHAIN`, which addresses these issues and ensures security, fairness, trust, and interoperability among all participating entities. Our work is built on well-established technologies that are assembled into a novel architecture. The backbone of our proposed architecture is Blockchain, providing data transparency, traceability, and fostering applications for the evolution of cyber insurance. `INCHAIN` includes two applications: *Smart Contracts* and *Self-Sovereign Identity (SSI)*. Smart Contracts equip `INCHAIN` with automated tasks and requirements that bind participating entities, while SSI enables data minimization, robust identification, data interoperability, portability, controllability, decentralization, and transaction transparency. Our proposed architecture provides a viable solution to the rigid cyber insurance ecosystem by proving the benefits and demonstrating how it can address these challenges.

In summary, we make the following main contribution:

- We provide a comprehensive overview of the challenges plaguing the cyber insurance ecosystem.
- We conduct an in-depth analysis of existing research that leverages Blockchain and Smart Contracts to address the cyber insurance challenges.
- We propose a novel and comprehensive architecture, titled `INCHAIN`, that integrates Blockchain, Smart Contracts, and SSI technologies to tackle the challenges the cyber insurance industry faces.
- We evaluate the efficacy of our proposed architecture, analyzing its suitability for integration within the cyber insurance ecosystem and assessing its ability to address the identified cyber insurance challenges compared to existing research incorporating Blockchain and Smart Contracts.

The remainder of this article is structured as follows. Section 2 presents related work, summarizes cyber insurance challenges, and analyzes candidate technologies used in the proposed architecture. Section 3 elaborates on cyber insurance stakeholders, applied processes, and the proposed `INCHAIN` architecture, including involved operations. Next, Section 4 examines how `INCHAIN` meets cyber insurance processes, holistically addresses identified challenges, and compares `INCHAIN` with other works. Section 5 discusses the limitations of this paper and proposes directions for future work. Finally, Section 6 concludes the paper.

Table 1: Table of acronyms

Acronym	Definition
CIB	Cyber Insurance Broker
DID	Decentralized Identifier
IC	Insurance Company
NCSA	National Cyber Security Authority
PH	Policyholder
PHI	Protected Health Information
PII	Personal Identifiable Information
SSI	Self-Sovereign Identity
VC	Verifiable Credential

2 Background

This section first provides an overview of the acronyms used throughout the paper. It then delves into previous research on cyber insurance that utilizes Blockchain and Smart Contracts, outlines the challenges faced in cyber insurance, and analyzes the selected technologies that form the basis of the proposed architecture.

2.1 Acronyms

This paper employs several acronyms to refer to specific terms and concepts. We have included a table of acronyms to ensure clarity and avoid confusion. Table 1 offers a comprehensive list of all the acronyms used in this paper, along with their corresponding definitions. We encourage readers to consult this table whenever encountering an unfamiliar acronym in the text, as it will provide a quick reference to its meaning. By using acronyms judiciously and including a table for easy reference, we aim to make our paper more accessible and comprehensible to readers while maintaining the requisite technical terminology for our research.

2.2 Related Work

Franco et al. [10] introduced `SaCI`, a Blockchain-based approach that enhances trust and automation in the interaction between the PH and its IC. Their approach utilizes Smart Contracts to handle multiple aspects of the cyber insurance process. These contracts facilitate premium payments, contract updates, damage coverage requests, dispute resolutions, and contract information and integrity verification. The authors evaluated the effectiveness of `SaCI` through a proof of concept in dispute cases. `SaCI` is implemented on the Ethereum network, where each Smart Contract function incurs a gas fee. To further support this endeavor, Lepoint et al. [11] proposed `BlockCIS`, a dynamic cyber insurance system that collects data on the PH's information technology and computer infrastructure. This data is used for tailored risk assessment and attack surface identification. Third parties and auditors can access the collected data for analyses and actions. `BlockCIS` is developed on top of the Hyperledger Fabric, eliminating fees for executing Smart Contract functions.

Vakilinia et al. [12] presented a Blockchain-based cyber insurance crowdfunding framework on the Ethereum network. This framework involves four participants: Vendor, Customer, Auditor, and Insurance Company. The insurance process begins with the vendor requesting insurance services. Interested insurers then participate in a sealed-bid auction, submitting their preferred premium for the insurance service. The auction winners are selected to provide insurance coverage. In case of an indemnity request, an auditor verifies its validity. The authors implemented the proposed system on the Ethereum Blockchain, resulting in gas fees. The developed Smart Contract handles crowdfunding initialization, bidding, wrapping, and reimbursement.

Xu et al. [13] enhanced the time efficiency of crowdsourcing tasks in Blockchain applications. The proposed framework reveals its robustness through three different time-relative tasks: (*i*) time-sensitive, (*ii*) slightly time-sensitive, and (*iii*) time-insensitive. Automation of tasks in reimbursement issues is achieved within this framework. The authors developed the framework on the Ethereum network, where each Smart Contract function incurs a gas fee. The Smart Contract handles various actions, including bidding, cyber insurance creation, and reimbursement.

The `SECONDO` project [14] introduces a dedicated platform for the assessment and effective management of cyber risks, adopting a quantitative approach that considers both technical and non-technical parameters, such as user behavior, which influence cyber exposure. It aims to address information asymmetry between the insured and the insurer while providing analysis for efficient risk management by recommending optimal investments in cybersecurity controls [15]. The project determines residual risks, estimates cyber insurance premiums based on the IC's business strategy, and eliminates information asymmetry between the PH and the IC [16]. To securely store data on the effectiveness of implemented cybersecurity controls, `SECONDO` integrates the Blockchain technology and utilizes Smart Contracts embedded in the distributed ledger. These Smart Contracts automate agreement processing, notify the ICs and PHs when an agreement is bound, and facilitate premium and commission payments.

Blockchain has been employed in various insurance-related business cases. Loukil et al. [17] proposed CioSy, a collaborative blockchain-based insurance system that

monitors and processes insurance transactions. It utilizes smart contracts for claims handling, payments, and validation, and is built on top of the Ethereum, resulting in gas fees for its operations. Kumar et al. [18] presented FLAME, a trusted fire brigade service and insurance claim framework that utilizes blockchain to offer immediate fire brigade services and prevent insurance fraud. The authors provided the architecture and functionality of FLAME, where smart contracts automate the processes related to fire brigade services and insurance claims. The prototype has been implemented on the Hyperledger Besu Blockchain, using the Istanbul Byzantine Fault Tolerance 2.0 consensus protocol.

Yadav et al. [19] proposed a blockchain framework for vehicle insurance to streamline the reporting of accidents and filing of insurance claims. The framework is developed on top of the Hyperledger Fabric to store information about vehicles, owners, and insurance. Efficient querying of this blockchain requires specific participants, assets, and transactions. The consensus algorithm identifies invalid claims if a transaction request contains an error. Karmakar et al. [20] proposed ChainSure, an Ethereum blockchain-based framework empowered with TOPSIS and smart contracts, which provides an automated, tamper-proof, transparent, and scalable system fulfilling the major functional blocks in a medical insurance environment. ChainSure using the TOPSIS method allows users to find an insurance policy that best suits their needs. ChainSure has also gas fees.

In essence, the utilization of Blockchain and Smart Contracts within the insurance ecosystem has been already proposed in previous works focusing on various insurance sectors including but not limited healthcare insurance, cyber insurance and vehicle insurance. The works [10–14] have utilized Blockchain and Smart Contracts in business cases dedicated to cyber insurance. However, and to the best of our knowledge, SSI has not been integrated by any existing work in the literature. So far, Blockchain-based cyber insurance systems assist ICs in devising tailored insurance premiums, while PHs can validate that a cybersecurity incident is covered in the insurance policy, and perform transactions related to claims' handling with minimal effort and delays.

2.3 Challenges

Cyber insurance is a hybrid ecosystem combining features from classic insurance and information technology and inherits challenges from both sectors. The existing literature analysis has identified numerous challenges the cyber insurance ecosystem faces, which we present below. We tackle here the first research question (*RQ1 – Which are the main insurability challenges?*).

CH1 – Lack of Data. The cyber insurance ecosystem requires plenty of data to perform an accurate cybersecurity risk assessment and a fair premium calculation. In particular, the data needed is the following. The *historical data* for their potential PHs to identify future cyber-attacks [21]. The *data from the PH's industry* (e.g., healthcare, information, finance) that can reveal a set of asset vulnerabilities and the frequency of a cybersecurity incident occurrence. The *general cybersecurity data* related to information systems (i.e., network, operating systems, information security management system), processes, and human resources for the specific PH. Sadly, ICs do not share their collected data with others due to technical and legal obstacles, as well lack of trust in such a competitive market.

CH2 – Lack of Automated Tasks. All processes between ICs and their PHs require manual operations and labor, which are highly time-consuming [14, 22]. The most critical processes, the claim's submission and validation, are the most time-consuming and drawn-out ones; ICs have to process the claim, verify the cybersecurity incident, and decide whether the PH qualifies for reimbursement.

CH3 – Fraudulent Claims. The most important risk of an insurance agency is the fraudulent actions by PHs [23, 24], which insure their cyber assets at many ICs. This approach allows a dishonest PH to make multiple claims to different ICs for the same cybersecurity incident or split the claims and over-represent losses from the same one [25].

CH4 – Identity Theft. Attackers submit false claims masquerading eligible PHs to an IC utilizing various social engineering techniques, including but not limited to phishing attacks and stealing the personal information of PHs [13,26,27]. Remarkably, this challenge originated from ineligible PHs.

CH5 – Loss of Sensitive Data. ICs store the gathered data becoming vulnerable to cybersecurity attacks that aim to copy, alter, or delete them [28, 29]. These are personal data, including the PH's revenue, its assets inventory, its answers to risk assessment questionnaires that prove vulnerability existence, and a set of scanned paper credentials. Data breaches in ICs can expose PHs' personal data that can be used for various cybersecurity attacks (i.e., masquerade). Therefore, rigid data storing methods by ICs inhibit the expansion of the cyber insurance market. Apart from that, PHs may also be targeted by malevolent attacking groups that pretend to be legal ICs to steal their sensitive data and perform illegal actions.

CH6 – Know Your Customer. This challenge includes the actions that ICs follow to verify the identity of PHs and monitor their behavior before and during the life of the cyber insurance contract. ICs request that PHs provide detailed and updated information about their businesses. The existing verification methods are costly and time-consuming. In addition, the quality of the collected data may be inaccurate, leading ICs to draw the wrong conclusions for them [30, 31].

CH7 – Information Asymmetry: It refers to a market situation in which one party has insufficient information about the other party, leading to market failure [32]. Information asymmetry is directly connected to moral hazard and adverse selection. On the one hand, moral hazard occurs when the PH gets involved in a risky event knowing its protection against the risk and the IC will pay the cost [2, 33, 34]. That means one of the parties (usually the PH) accepts a deal to change its behavior after a deal is made. This happens when it believes it will not have to face the negative consequences of its actions. On the other hand, adverse selection occurs when the PH conceals its high-risk exposure from the IC before the cyber insurance contract [2, 33, 35]. That means one of the two parties has more accurate or different information than the other before they reach an agreement. This puts the less knowledgeable party at a disadvantage because it is more difficult for it to assess the risk of the deal. Overall, this ultimately leads to an inefficient outcome and a lower quality of goods and services in the market.

Apart from the challenges above, others, such as *Interdependent and Correlated Risks*, and *Premium Calculation*, have been studied and addressed. Regarding the Interdependent and Correlated Risks, they are created during the cybersecurity risk assessment due to the connectivity of information assets of a PH with other assets on an external network [36, 37]. As for the Premium Calculation, their existing formulas are static and unable to adopt technological changes to reduce the overpricing of cyber insurance [38]. On the contrary, the present work avoids getting involved with the aforementioned cyber insurance challenges (i.e., Interdependent and Correlated Risks, and Premium Calculation) since these cannot be addressed with the existing characteristics of Blockchain, Smart Contracts, and SSI (technologies that comprise the proposed cyber insurance architecture, see Section 2.4).

2.4 Candidate Technologies

At this point, we present the technological pillars of the proposed cyber insurance architecture. These jointly provide a robust solution for the cyber insurance ecosystem and analyze why the proposed architecture integrates them. Also, the proposed architecture has been designed on the grounds of well-established technologies (i.e., Blockchain, Smart Contracts, and SSI) with proven security properties.

2.4.1 Blockchain

Blockchain lies in the concept of distributed ledgers that assist in making a log of any asset's history that cannot be altered and is transparent for all involved entities to check [39]. Blockchain is the crux of the proposed architecture, not as a stakeholder but as a network. It will not only enable trust, security, transparency, and the traceability of data shared across a business network, but it will also create a fertile surface for applications that will support the cyber insurance processes. The proposed cyber insurance architecture takes advantage of the following Blockchain features [40]: (*i*) immutability, (*ii*) distribution, (*iii*) decentralization, (*iv*) secure records, (*v*) consensus, and (*vi*) unanimity.

2.4.2 Smart Contracts

A Smart Contract is a contract between two or more Blockchain nodes [41]. They are programs stored within a Blockchain that respond to certain events encoded within the contract. In essence, they are responsible for automating the execution of an agreement so that its participants remain assured of the outcome without any intermediary's intervention. Smart Contracts follow the "`if/when ... then ...`" statements and can automate a workflow by triggering an upcoming action when predetermined conditions are met. When these conditions are met and verified, the Blockchain nodes execute the actions and update the Blockchain. Therefore, the transaction is immutable. Thus, only nodes with the right permissions can see the results. The proposed cyber insurance architecture takes advantage of the following Smart Contracts features [42]: (*i*) agreement, (*ii*) speed, (*iii*) automation, (*iv*) security, and (*v*) records management.

2.4.3 Self-Sovereign Identity

Self-Sovereign Identity [43, 44], also known as SSI, is a decentralised identity management system. It allows individuals or organizations to own and manage their digital identities. In addition, SSI facilitates the practice of selective attribute disclosure as a means of reducing the disclosure of personal data. Furthermore, it offers privacy-preserving characteristics such as *anonymity* and

unlinkability. With SSI, no central authority maintains possession of users' data, eliminating the need to pass it on to others upon request. The user carries its data, and due to the underlying cryptography and distributed ledger technology, it can make claims about its identity, which others can verify with cryptographic certainty.

By utilizing SSI, cyber insurance stakeholders can exchange verifiable data in an automated and privacy-preserving manner. This approach helps prevent the leakage of private information and saves time by eliminating the need for manual data verification processes. At the heart of SSI lie the Verifiable Credentials (VCs). W3C published a formal recommendation of VCs and defined them as tamper-evident credentials with authorship that can be cryptographically verified [45]. VCs are interoperable and support selective disclosure of its user's information. In general, the engaged participants in SSI are an issuer, a user (the one who owns the VCs), and a verifier. The SSI is comprised of two basic functionalities: (*i*) *VC Issuance* and (*ii*) *VC Verification*.

The first functionality is the VC Issuance, where the user (acting as the holder) acquires a VC from the issuer. VC consists of tamper-evident claims and metadata that cryptographically prove its issuer [45]. Claims represent a holder's statements (e.g., the number of past data breaches). Each VC is issued on its holder's and issuer's Decentralized Identifiers (DIDs) and has the role of a public key. A DID is a globally unique persistent identifier that consists of a string of letters and numbers and is directly correlated with a pair of public and secret keys. The private key allows the user to access and manage its data. The user should be the only one who knows the private key, which should never be shared with anyone else. Regarding DIDs, the private key allows users to prove ownership and grant permission to share specific data. On the other side, Blockchain stores the public key associated with the DID of the VC's issuer public key and is safely shared with anyone to send and receive data. A digital identity wallet securely stores the issued VCs [46]; it is the place (e.g., a mobile app) where holders keep their VCs [47]. These cannot be hosted only within smartphones; some implementations support their host within trusted computers [48–50].

The second functionality is the VC Verification, in which the user (acting as the prover) must demonstrate possession of accurate attributes to the verifier without necessarily revealing the values contained within them. This is accomplished using zero-knowledge proofs and establishing that the corresponding user is, in fact, in control of the presented identity. To verify the authenticity of the VC, the verifier shall check the Blockchain to see its issuer (i.e., DID of the VC's issuer) without having to contact the issuer. When presenting a VC, the user can select which claims to disclose and which to conceal. In addition, SSI achieves unlinkability as the user employs a distinct DID for each presentation.

SSI is built on top of Blockchain and equips the proposed cyber insurance ecosystem with trust among the participants, instant exchanged data verification, robust identification, data minimization, interoperability, portability, controllability, decentralization, and transaction transparency. The proposed cyber insurance architecture integrates the SSI due to its following features [43]: (*i*) less personal data management, (*ii*) transparency, (*iii*) interoperability, (*iv*) decentralized identity management, and (*v*) instant verification.

3 The Cyber Insurance Concept

This section outlines the fundamental stakeholders and processes that constitute the existing cyber insurance ecosystem while analyzing the participants and operations of the proposed architecture, called `INCHAIN`, designed to tackle cyber insurance challenges.

3.1 Definition, Stakeholders, and Processes

Here, we address the third research question (*RQ3 – Which are the basic stakeholders, processes of cyber insurance, and how do they interact to accomplish the goal of cyber insurance?*). The essential stakeholders in cyber insurance are further elaborated below [33, 51, 52]. In a nutshell, a PH is a holder of cyber insurance and a customer to an IC. The latter is a stakeholder responsible for selling cyber insurance policies to potential PHs, investigating a cybersecurity incident, and auditing whether the PHs comply with the cyber insurance policies and have implemented the indicated cybersecurity countermeasures [23]. Additionally, Cyber Insurance Brokers (CIBs) performi market research and bring the most suitable contracts to their PHs. We analyze the identified cyber insurance processes below:

CIP1 – Market Research: A CIB aims to find advantageous cyber insurance contracts for its PHs [52]. The latter knows its cybersecurity exposure and has already identified the cybersecurity risks; technical measurements will address some of them [15, 49, 53] and cyber insurance contracts will cover them in a cybersecurity incident. During this phase, the CIB thoroughly explains the available cyber insurance policies to its PHs, analyzing its definitions, liabilities, coverages, and exclusions. The latter is written in a boilerplate language and comes with many disadvantages, including but not limited to a misunderstanding about what is insured,

what perils and risks are covered, and how losses are assessed [16, 54, 55]. This process is performed between a CIB and a potential PH. The *Market Research* process is performed between a CIB and a PH, and it is directly related to the *Information Asymmetry* (*CH7*) since a PH has to understand what each cyber insurance contract can offer to meet PH's requirements. However, in this process the IC is not involved and the candidate technologies (see Section 2.4) cannot address it. Thus, its optimization is outside the scope of this work.

CIP2 – Client Registration and Validation: On the one hand, the potential PH gathers the required documents to register and apply for a cyber insurance contract with its IC. These include but are not limited to identification documents, IT security certifications, and any other compliance documents [56, 57]. On the other hand, the IC verifies the validity of the applied documents [14, 57]. It also verifies their accuracy. Once the validation is complete, the PH can carry on safely, knowing that it is fully insured. This process is performed between an IC and a potential PH. It is well known that processes responsible for validating and registering a PH lack unmanned actions (`CH2`). Currently, the existing actions are time-consuming and require human labor. Dishonest PHs also deceive ICs by submitting outdated documentation (`CH6`) regarding their status (e.g., updated security controls). Finally, ICs store data related to PHs becoming vulnerable to cybersecurity attacks (e.g., data breaches) and being at risk of losing personal data (`CH5`).

CIP3 – Underwriting: It is the most crucial process for the IC and is based on assessing the cybersecurity risk of the PH [33, 58]. First, the IC identifies the main parameters of risk considering valuable assets, possible threats, and existing vulnerabilities of the PH. Then, the IC determines an incident's likelihood and possible impact, considering the combined probability of events happening. A blend of self-assessment questionnaires, checklists, business documentation, meetings, as well as interviews perform this assessment [15, 59–61]. Their main goal is to pinpoint the installed software and deployed security measures, and verify the existence of sensitive data and how it is accumulated and handled. It undoubtedly aims to detect any other information that can affect the global security posture of the firm under investigation [62]. A deeper analysis can be carried out by installing monitoring software that produces security logs and telemetry devices. The results of this process contain analysis and advice of the PH, emphasizing deficiencies and precautions to comply with the well-known and top-notch security practices [63]. Also, the IC may suggest and demand the implementation of security countermeasures [64], which will affect the premiums [65–67]. This process is performed between an IC and a potential PH. The weakness of this process is the lack of automated tasks (`CH2`) to validate if PHs have fulfilled the IC's requirements and propositions (`CH6`). Currently, the compliance of PHs with IC's requirements is validated through questionnaires and audits. PHs can exploit that backdoor by submitting inaccurate data (`CH7`).

CIP4 – Pricing Premium: An IC is in charge of calculating the price of the PH's premium using existing econometric and statistical models [35, 38, 58]. This process is performed between an IC and a potential PH. It is observed that the lack of historical cybersecurity data is of utmost importance [38]. Data can influence the premium calculation with parameters that may be a barometer for the final price; however, lack of data leads to unfair premiums (`CH1`). This process is outside the scope of this work. Thus, we do not design and deliver an algorithm to optimize this process.

CIP5 – Periodic Risk Assessment: Risk assessment is highly recommended and conducted by the IC during a cyber insurance lifetime [33]. It allows ICs and PHs to collect updated information about new threats, vulnerabilities, and evolving cyber risks. Overall, it is required to perform a continuous risk assessment to reduce the amount of PHs' impassable information, with the ultimate goal being to mitigate unfair behaviors such as negligence and fraud. An IC and a PH perform this process. Until now, this process has been mainly conducted through questionnaires. Thus, the absence of automated methods (`CH2`) to collect accurate cybersecurity data makes this process vulnerable to cybersecurity attacks performed by legal PHs that aim to fool it by answering spuriously in questionnaires (`CH6`). As a result, IC has an inaccurate view of PHs' cybersecurity exposure (`CH7`).

CIP6 – Claims Submission: As soon as a PH realizes a cybersecurity incident occurrence, it informs its IC to request reimbursement [58]. This step aims to get a refund to cover damages from the cybersecurity incident. Generally speaking, cyber insurance protects a PH through three distinct insuring agreements: (*i*) *Network Security and Privacy Liability*, (*ii*) *Media Liability*, and (*iii*) *Errors and Omissions* [68]. The PH has to fill out documents describing the cybersecurity incident in detail, including but not limited to information related to the location, hour, infected systems, networks, software, damaged hardware, downtime of systems, the type of compromised data (personal or not), as well as the estimation of potential economic losses [69]. This process is performed by a PH. Currently, the claim sub-

mission process is time-consuming and requires human labor (e.g., sending documents through email and filling out questionnaires). When this procedure is done, a significant amount of time will have been wasted in addressing the problem on the PH's side. Automated claim submission processes can solve this issue. Also, the lack of a robust identification system within the cyber insurance ecosystem leads ICs to face dishonest PHs that seek reimbursement without any incident and malevolent actors that masquerade as eligible PHs to steal their reimbursement (CH2, CH3, and CH4).

CIP7 – Claims Validation and Auditing: IT security experts from the IC start verifying the claim's submission and performing a forensic investigation [58, 70, 71]. Notably, most policies in a cyber insurance contract cover the cost of incident response and forensic investigations, including identifying stolen or compromised data and the extent to which third parties have to be informed according to the current regulations. Audits performed by the IC aim at revealing a PH's fraudulent claim or a PH that does not follow the reported security procedures. In this case the IC can refuse to indemnify the PH [23]. This process is performed between an IC and a PH, and requires human involvement. Validation and auditing are time-consuming due to a lack of automated methods for gathering accurate and real-time cybersecurity data (CH2 and CH6). Audits last for an extended time. Hence, until its completion, the victim (PH) may have already lost money and reputation. In certain cases, the responsibility for incident response does not lie with the IC, but rather, the PH opts to engage an external firm to detect, mitigate, and recover from the cybersecurity incident. This proactive measure aims to minimize the impact and losses resulting from such incidents. The expenses incurred for incident response services provided by external firms are referred to as *transaction costs* and are ultimately covered by the PH [72].

CIP8 – Claims Payment: It is the final stage of the cyber insurance life cycle, and reimburses the PH due to the cybersecurity incident [73]. The refund reimburses the PH's business not only due to interruption caused by a cybersecurity incident but also due to loss of reputation whenever the cyber incident is publicly disclosed [74]. This process is performed between an IC and a PH. It is well-known that the lack of automated payments transforms this process into a stiff one (CH2).

In summary, based on the analysis above, the following observations are raised. First and foremost, the *Market Research* process is influenced only by *CH7* challenge. The process named *Client Registration and Validation* is affected by the CH2, CH5, and CH6 challenges.

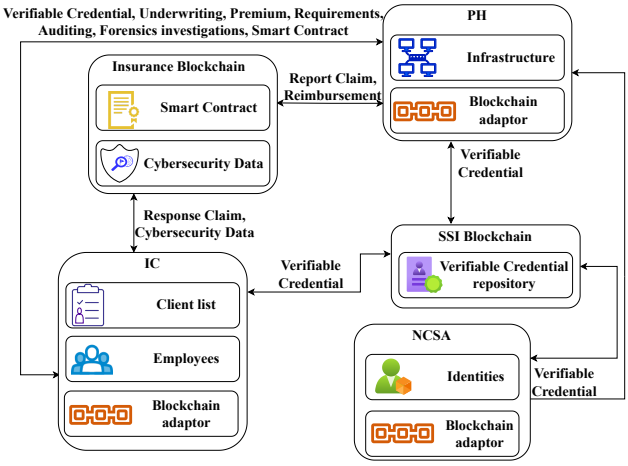

Figure 1: INCHAIN architecture

Next, the *Underwriting* process is influenced by the CH2, CH6, and CH7 challenges. Moreover, the *Pricing Premium* process is affected by the CH1 challenge. Furthermore, the *Periodic Risk Assessment* process is afflicted by CH2, CH6, and CH7 challenges. The *Claims Submission* process is affected by the CH2, CH3, and CH4 challenges. The *Claims Validation and Auditing* process is directly related to CH2 and CH6 challenges. Finally, the *Claims Payment* process is influenced by CH2 challenge. Table 2 depicts the aforementioned observations.

3.2 INCHAIN

We introduce here the cyber insurance architecture of INCHAIN, including the operational layer of every participant (see Figure 1). The engaged participants are analyzed in detail:

NCSA: This entity is newly introduced in this paper as a pillar of the proposed cyber insurance architecture. It constitutes an SSI issuer, allowing potential PHs to issue VCs (see Section 2.4.3) from their verified identity attributes and then use them to access cyber insurance services. A National Cyber Security Authority (NCSA) coordinates activities with all ministries, government agencies, and bodies, ensuring interoperability at all levels and and has the ability to issue VCs with accurate data for each possible PHs. Furthermore, it has a Blockchain adaptor to upload the issued VCs to the Blockchain. NCSA communicates only with potential PHs and the SSI Blockchain network. In addition, NCSA maintains all data pertaining to recent cybersecurity events with PHs, which is mandadory for generating accurate VCs. In essence, adding a new entity responsible for issuing VCs is inevitable; none of the existing stakeholders is confident enough to issue VCs

Table 2: Correlation between cyber insurance challenges and processes

Challenges	Processes							
	CIP1	CIP2	CIP3	CIP4	CIP5	CIP6	CIP7	CIP8
CH1 - Lack of Data	✗	✗	✗	✓	✗	✗	✗	✗
CH2 - Lack of Automated Tasks	✗	✓	✓	✗	✓	✓	✓	✓
CH3 - Fraudulent Claims	✗	✗	✗	✗	✗	✓	✗	✗
CH4 - Identity Theft	✗	✗	✗	✗	✗	✓	✗	✗
CH5 - Loss of Sensitive Data	✗	✓	✗	✗	✗	✗	✗	✗
CH6 - Know Your Customer	✗	✓	✓	✗	✓	✗	✓	✗
CH7 - Information Asymmetry	✓	✗	✓	✗	✓	✗	✗	✗

with accurate claims, in contrast to NCSA, which accomplishes this with high confidence.

PH: Apart from the characteristics reported in Section 3.1, the PHs of INCHAIN is equipped with the following capabilities. The PH makes a request to the NCSA to issue VCs based on its attributes. Hereafter, the PH submits the VCs to the IC to purchase cyber insurance to safeguard its infrastructure that satisfies IC's criteria. Moreover, it is geared with a Blockchain adaptor to create a Smart Contract together with the IC—describing in a digital format the agreed cyber insurance contract—as well as to report a cybersecurity incident.

IC: Apart from the characteristics defined in Section 3.1, the IC of INCHAIN is also equipped with the following attributes. The IC is a VC verifier verifying the received credential of a potential PHs, checking the latter's eligibility to use the service (cyber insurance). Furthermore, it is equipped with a Blockchain adaptor to create Smart Contracts together with PHs to handle cybersecurity claims and store cybersecurity data to monitor its behavior via the Smart Contract.

SSI Blockchain: This Blockchain network belongs to the NCSA. It is responsible for storing VCs and performing operations related to their issuance and verification (see Section 2.4.3).

Insurance Blockchain: This Blockchain consists of pre-selected ICs, which are responsible for validating transactions and have banded together to share information to improve existing workflows, transparency, and accountability. It is responsible for storing Smart Contracts and processing claims.

INCHAIN allows a PH to completely control its cyber insurance contract. The basic scenario of INCHAIN unfolds as follows. A possible PHs is a legitimate business and is exposed to cybersecurity threats. At some point, the PH aims to buy a cyber insurance contract from its desirable IC. The latter has specific requirements to sell its cyber insurance contracts. Thus, based on them, IC will calculate the premium of PH's cyber insurance contract and perform a continuous risk assessment to prevent naive behaviors and fraud. The requirements are the following:

1. ***Business Information:*** It includes information related to the legal business name, its principal address, business nature (e.g., SME), number of employees, and annual audited revenue.
2. ***Type of Collected Data***: It includes information related to the type of data that the business processes and stores (e.g., Personal Identifiable Information (PII), Protected Health Information (PHI), intellectual property).
3. ***Security Controls***: These include information related to compliance with cybersecurity certifications (e.g., ISO27001, GDPR), utilization of *Payment Card Industry Data Security Standards*, and integration of cybersecurity controls (e.g., IDS, firewall, IPS).
4. ***Information Loss***: It includes the number of past data breaches (e.g., the PH has totally faced seven data breaches).

INCHAIN is an architecture that benefits both ICs and PHs. A notable advantage of INCHAIN is the automated verification process of attributes and claims handling for the cyber insurance ecosystem. In essence, PHs get reimbursed immediately since the Smart Contracts transfer money from one account to another without the involvement of third parties. Therefore, the PHs can immediately focus on recovering from the incident. Finally, Smart Contracts are also responsible for monitoring PHs' behavior (e.g., contract violation) via the collection of cybersecurity data (e.g., audits).

3.3 INCHAIN Operations

INCHAIN consists of the following individual operations: (*i*) *Verifiable Credential Issuance*, (*ii*) *Verifiable Credential Verification and Cyber Insurance Issuance*, and (*iii*) *Cybersecurity Incident Report and Reimbursement.* The INCHAIN architecture does not include actions involving the selection of a cyber insurance contract between a potential PH and CIB and the premium pricing. These operations are inextricably linked in the cyber insurance backbone; however, they are outside the scope

Table 3: Cyber insurance contract requirements and claims

Attribute	PH (Attribute)	IC (Requirements)
Business Information		
Name	INCHAIN Tech	Official Name
Address	Milky Way 21	Existing Address
Business Nature	Information Technology	ALL types
Number of Employees	50	<50, 50-100, 100+
Annual Audited Revenue	210K €	<250K, 240K-500K, 500K+
Type of Collected Cata		
Type of Stored Data	PII	ALL
Type of Processed Data	PII	ALL
Security Controls		
Certifications Compliance	ISO27001, GDPR	At least one
Security Controls	IDS, firewall, backup	Last update < today
Information Loss		
Number of Past Data Breaches	7	<10
Total Fines	7K €	<1M €

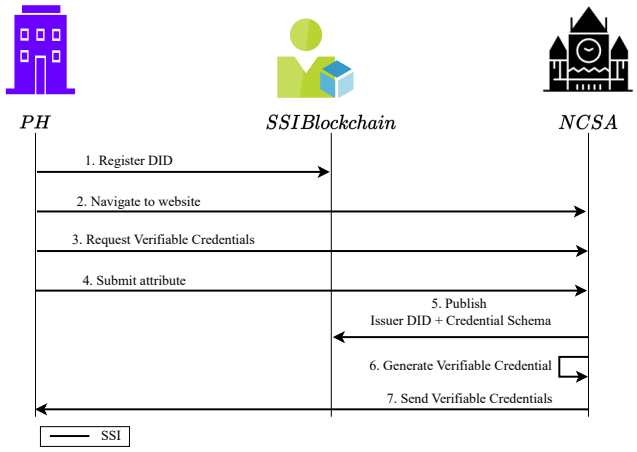

Figure 2: INCHAIN Verifiable Credentials issuance

of this work. Below, each INCHAIN operation is examined together with its purpose, its relationship to existing cyber insurance processes (see Section 3.1), and how it addresses specific cyber insurance challenges (see Section 2.3). The INCHAIN operations are analyzed based on IC's requirements for selling cyber insurance contracts and a PH's attributes; Table 3 represents both of them.

3.3.1 Verifiable Credential Issuance

As its name implies, this operation is responsible for issuing VCs to a PH based on its verified attributes. It is executed between a PH and a NCSA. It aims to create a robust identification method for supplying the IC with the PH's accurate data. In particular, this operation enriches the traditional cyber insurance process entitled *Client Registration and Validation* with automated mechanisms. These are responsible for equipping PHs with verified data by NCSA that do not demand human intervention for their validation by ICs.

For the credential issuance (see `Steps 1 - 7` depicted in Figure 2), let us assume that the potential PH uses a secure identity wallet on its trusted device (see Section 2.4.3). At the beginning of the VC issuance procedure, PH generates a public/private key pair, stores the private key within its trusted device, and publishes the public key to the Blockchain, generating and storing its DID for the public key in its data store (`Step 1`). Then, the PH navigates to the NCSA website and requests from it to issue the VCs (`Steps 2 - 3`). PH requests the issuance of the following four VCs:

- ***Business-Information-VC*** that includes PH's official name, address, business nature, number of employees, and its latest annual audited revenue, along with their legitimacy proofs.
- ***Type-of-Collected-Data-VC***, which proves that the PH stores and processes only PII data.
- ***Security-Controls-VC***, which proves that the PH complies with ISO27001 and GDPR, and has installed all required security controls (i.e., IDS, firewall, backup policy routine).
- ***Information-Loss-VC*** that proves the PH has already been a victim of a cybersecurity attack at least seven times, and its total fine is 7K €.

The aforementioned four INCHAIN's VCs follow a specific format and include the subsequent attributes:

➢ ***ID*** that is a unique verifiable identifier characterizing the credential (e.g., *https://ncsa.gr/credentials/1872*).

➢ ***Credential Type*** that represents that the current credential is a verifiable one (e.g., *Business-Information-VC*).

➢ ***Issuer*** that represents the issuer who issued it (e.g., NCSA). It is a type of PH that explains PH's status, whether it is an individual or an enterprise (e.g., *Large Enterprise, SME*).

➢ ***Issuance Date*** that represents the VC's issuance date (e.g., `2022-31-12T00:00:00Z`).

➢ ***Lifetime*** that represents VC's expiration date (e.g., `2023-31-12T00:00:00Z`).

➢ ***Proof*** that represents the public key signatures of the PH's and NCSA's DID. This information will be used later by the IC to verify the authenticity of the identity and claim by verifying the PH and NCSA's DID signatures (contained in the claim) against the verifiable data registry. The Proof contains the following fields:

- ***Type:*** The specific type of the proof's signature (e.g., `Ed25519Signature2020`)
- ***Created Date:*** The day of the proof's creation (e.g., `2022-31-12T00:00:00Z`)
- ***Verification Method:*** The method that should be used for verification by the verifier (e.g., *selective disclosure*)

- ***Proof Purpose:*** The purpose for the proof (e.g., *assertionMethod*)
- ***Proof Value:*** The value of the specific proof (e.g., *z58DAdFfa9SkqZMUJ*)

➢ ***Claim*** that includes identity attributes for the PH (e.g., number of past data breaches). The Claim includes the following fields:

- ***Identifier:*** The unique attribute identifier of the VC: (e.g., `did:ebfeb1f712ebc6f1c276e12ec21`)
- ***Attribute:*** The owner's identity attribute (e.g., number of past data breaches: 7)

NCSA, as part of the public sector, collects the verified data from other ministries, government agencies, and bodies and issues the *Business-Information-VC* and the *Information-Loss-VC*. However, for issuing the *Type-of-Collected-Data-VC* and *Security-Controls-VC* the PH submits its attributes to the NCSA for verification (`Step 4`). The submitted attributes are certifications proving that the PH complies with the `ISO27001` and `GDPR` and the latest security update occurrence issued by known organizations (e.g., the service provider). Upon successful verification, the NCSA publishes its DID and the credential schemas[1] of VCs to the SSI Blockchain and then issues VCs that are signed by its DID (`Steps 5 - 6`). Ultimately, NCSA sends the generated VCs to the potential PH. The latter stores them within its secure digital identity wallet and fully controls them (`Step 7`).

It is observable that this operation addresses the challenges `CH2` and `CH6`. SSI facilitates the *Know Your Customer* operations. Its usual responsibilities are performed automatically when a PH uses a SSI login (e.g., digital evidence of identification or other attributes are sought and delivered as part of the login process). Therefore, telephone verification and the provision of scanned papers are rarely required. Overall the multiple-step and time-consuming *Know Your Customer* processes are replaced with a SSI single, seconds-long procedure, which benefits both the IC and the PH.

3.3.2 Verifiable Credential Verification and Cyber Insurance Issuance

In this operation, the PH presents its VCs to the IC, and if the verification is successful, the PH can start using the cyber insurance services provided by the IC. A Smart Contract is used to translate the classic cyber insurance contract into a digital format, which binds the PH and the IC under specific requirements. This operation affects the traditional cyber insurance processes entitled `CIP2` and `CIP3`. On the one hand, the `CIP2` process on the IC side becomes fully automated due to the utilization of SSI and VCs. Hence, the PH will submit to IC only verified attributes minimizing the time needed for their verification since these will come from trusted entities (e.g., NCSA) and encapsulated within VCs. On the other hand, the `CIP3` process is strengthened by using VCs, as the IC's underwriters can gather verified information about the PH's cybersecurity awareness, behavior (e.g., number of past data breaches), and infrastructure. This leads to the identification of new cybersecurity risks that may not have been previously considered and could potentially affect the PH.

When the potential PH aims to buy a cyber insurance contract from a specific IC, it has to provide the VCs to the latter for validation (see `Steps 1 - 13` depicted in Figure 3). To initiate the operation, the potential PH interacts with its chosen IC by visiting the latter's website and requesting to buy cyber insurance (`Step 1`). The latter requests proofs (`Step 2`) based on specific requirements (see Table 3) from the potential PH proving that: (*i*) PH is a legitimate business, (*ii*) PH processes and stores data, (*iii*) PH complies with cybersecurity certificates and standards, (*iv*) PH has updated cybersecurity controls, (*v*) PH's total past data breaches are less than or equal to 7, and (*vi*) PH's total fine is less than 1M €.

Next, the PH selects and sends the whole claim or only a subset of it, ensuring minimal disclosure of data (`Step 3`). The proving function requires the participating entities to agree on which attributes will be disclosed (e.g., number of past data breaches) and which attributes will be partially revealed (selective disclosure) [76]. For more information see Table 3. For instance, apart from its annual audited revenue, the PH reveals the general information related to its business, the type of data stored and processed, and the information related to its implemented security controls. Regarding the annual audited revenues, the VC, instead of revealing the accurate value, responds with a `YES` as a positive answer, proving the PH's latest annual audited revenue is less than 250K €. Moreover, the PH hides information related to the number of past data breaches and the total fines; the VC, instead of revealing the accurate number of data breaches, responds with a `YES` as a positive answer, proving that the PH meets the requirement of having fewer than 10 data breaches and that its fine is less than 1M €. Based on the submitted VCs of the PH, the IC can verify that the PH conforms to its policies regarding the purchase of cyber insur-

[1] The Credential Schema is a document that is used to guarantee the structure, and by extension the semantics, of the set of claims comprising a VC. A shared Credential Schema allows all parties to reference data in a known way [75].

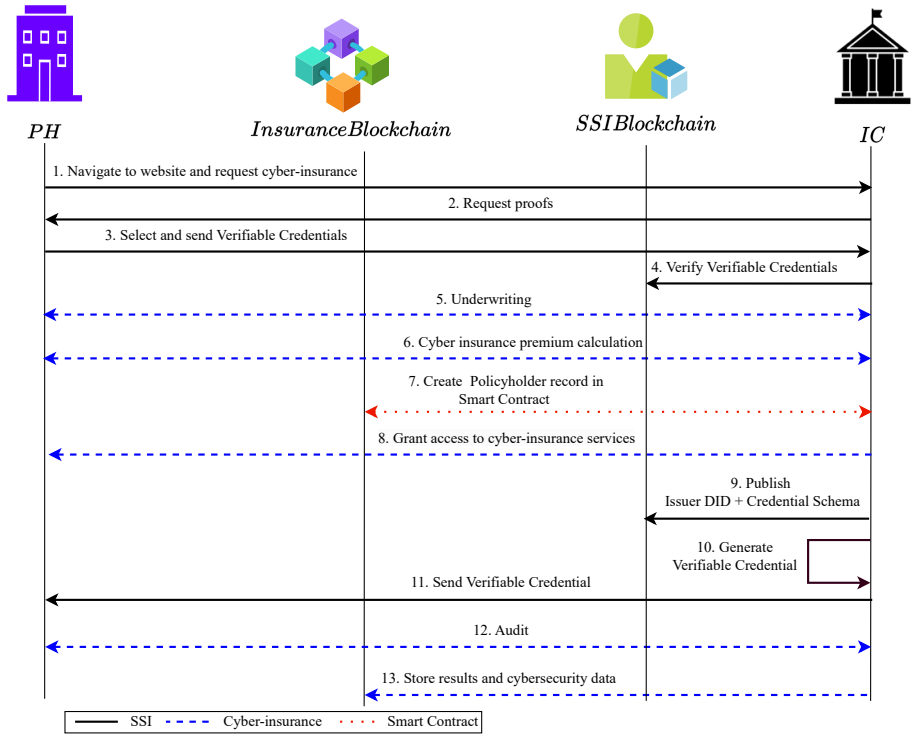

Figure 3: Verifiable Credential verification and Cyber-insurance issuance

ance; the IC validates the authenticity of the received VC by verifying the signatures of the PH's and NCSA's DID stored within the SSI Blockchain (`Step 4`).

Upon the successful verification, the IC, together with the PH, starts the processes related to underwriting and pricing the premium (`Steps 5 - 6`); the results of the previous actions lead to the cyber insurance contract agreement. Assuming that the cyber insurance premium is equal to 1080 €, the limit of liability[2] is at 591K € and the deductible[3] is 4K €. The cyber insurance purchased by the PH covers the incidents summarized in Table 4. In particular, PH is covered against business email compromise, lost device, malware/virus, phishing attacks, and ransomware cybersecurity attacks, with maximum reimbursement at 123K €, 57K €, 160K €, 72K €, and 179K € correspondingly (see Table 4). Then it is translated into a digital format as a Smart Contract binding them with specific requirements. Apart from the reimbursement information, the cyber insurance contract includes obligations that should be met by the PH (e.g., penetration tests every three months, daily vulnerability scanning and patching, and finally, two security awareness campaigns for its employees in a year). Moreover, the Smart Contract checks if the PH is consistent with its obligations during the coverage period. If the obligations above are not met by the PH, then the Smart Contract will be terminated, and in case of an incident, the PH will receive no reimbursement.

[2] The limit of liability determines the maximum amount of money an IC will pay for a covered claim.

[3] A deductible is the amount of money a PH must pay on its own before cyber insurance can cover the damages.

Table 4: INCHAIN covered cybersecurity incidents and maximum reimbursement

Incident Name	Maximum Reimbursement (€)
Business email compromise	123K
Lost device	57K
Malware/Virus	160K
Phishing	72K
Ransomware	179K

A record within the `INCHAIN` Smart Contract will include the following attributes:

- ***PH_{id}:*** A unique identifier characterizing the PH (e.g., `1531435435`).
- ***IC_{id}:*** A unique identifier characterizing the IC (e.g., `58567696`).
- ***Premium:*** The amount of cyber insurance contract (e.g., *1080 €*).
- ***Limit of Liability:*** The maximum amount an IC will pay for claims during the contract period (e.g., *500K €*).

- ***Deductible:*** The amount of money a PH must pay on its own before IC can cover the damages (e.g., *4K €*).
- ***Obligations:*** PH's obligations against the contract (e.g., *penetration tests every 3 months*).
- ***Reputation:*** A score characterizing the PH based on compliant behavior in obligations against the contract. Its initial value is equal to 100. If the PH violates the contract, its reputation decreases. The lower the value is, the worse the reputation is.
- ***Incident$_{id}$:*** A unique identifier of the incident and is correlated to specific incident evidence (e.g., firewall, IDS, IPG, and SOC logs) that are submitted by the PH and investigated by the IC.
- ***Incident:*** The name of the incident for which PH is requesting compensation (e.g., *phishing*).
- ***Reimbursement:*** The amount paid to cover expenses that have been spent due to the incident (see Table 4).
- ***Start Date:*** The contract's issuance date (e.g., `2022-31-12T00:00:00Z`).
- ***End Date:*** The contract's expiration date (e.g., `2023-31-12T00:00:00Z`).
- ***Coverages:*** The set of what cyber incidents PH is covered for (e.g *ransomware, business interruption, data breaches*).
- ***Controls:*** The set of installed PH's cybersecurity controls (e.g., staff cyber security training every six months).
- ***ExternalFirm$_{id}$:*** A unique identifier of the external firm that is responsible for handling the incident.

The `INCHAIN` Smart Contract consists of the following functions:

➢ ***PH Creation:*** It creates the PH record into the IC's Smart Contract within the Insurance Blockchain network. Its input is the values of PH_{id}, IC_{id}, *Premium*, *Limit of Liability*, *Deductible*, *Start Date*, and *End Date*. Its output is a new record that includes the data above.

➢ ***PH Reading:*** It returns the PH's cyber insurance contract stored in the Insurance Blockchain. Its input is the values of PH_{id} and IC_{id}. As output, it returns the value of PH_{id}, IC_{id}, *Premium*, *Limit of Liability*, *Deductible*, *Start Date*, and *End Date*.

➢ ***Incident Report:*** It is executed by the PH to report a cybersecurity incident. Its input is the value of PH_{id}, IC_{id}, $Incident_{id}$, and *Incident*. As output, it notifies the PH for the corresponding incident.

➢ ***Incident Response***: It is executed by the IC to accept or reject a reimbursement of a cybersecurity incident. Its input is the values of PH_{id} and IC_{id}. As output, it updates the value of *Limit of liability*.

➢ ***PH Obligation Checks:*** It is executed by the IC to check whether the PH meets its *Obligations* (e.g., penetration test every three months) comparing with *Controls*. Its input is the values of PH_{id} and IC_{id}. Its output is the value of *Obligations* together with a `YES/NO` that declares if the PH meets them or not.

➢ ***Asset Transfer:*** It can be called by the Incident Response function and transfers funds from IC to the PH. Its input is the values of PH_{id}, IC_{id}, and *Reimbursement*. As output, it notifies the PH that the asset has been successfully transferred to its account.

➢ ***Violation:*** It is triggered by the PH Obligation Check function, and it is responsible for decreasing the reputation of PH when the PH does not meet its obligations. Its output is the updated *Reputation* value.

➢ ***Contract Analysis***: It is triggered by both a PH and IC to present the incidents for which the PH is covered and its obligations with respect to those coverages. Its input is the values of PH_{id} and IC_{id}. Its output is the values of *Coverages* and *Obligations*.

➢ ***HandleIncident***: The Incident Response outsourcing occurs when the IC delegates the incident coordination to an external firm rather than handling it internally. The function takes inputs, including the values of IC_{id}, $Incident_{id}$, and $ExternalFirm_{id}$. The output of this function is an amount representing the transaction costs incurred, which will be factored into the final compensation calculation.

The IC creates a record within the Smart Contract for its new PH that is stored in the Insurance Blockchain (`Step 7`), and then, the PH can utilize cyber insurance services (`Step 8`). Moreover, the IC issues a VC to the PH to control the access to the *Insurance Blockchain* that consists of Smart Contracts and security information related to its PHs and handles all cyber insurance related (`Steps 9 - 11`). The VC issued by the IC verifies that the corresponding PH is the legitimate owner of the cyber insurance contract issued by it. Through this credential, the PH can access the Smart Contract stored within the Insurance Blockchain to perform actions regarding the cyber insurance contract, including but not limited to cybersecurity incident reports. Finally, the IC starts performing unexpected audits to the PH to identify Smart Contract violations and improve the data regarding this PHs that are stored within the Blockchain, achieving a continuous risk monitoring system (`Steps 12 - 13`).

Through this operation, `INCHAIN` addresses the cyber insurance challenges entitled `CH1`, `CH2`, `CH5`, and `CH6`. This `INCHAIN` operation is responsible for verifying PH's data against IC requirements to check its eli-

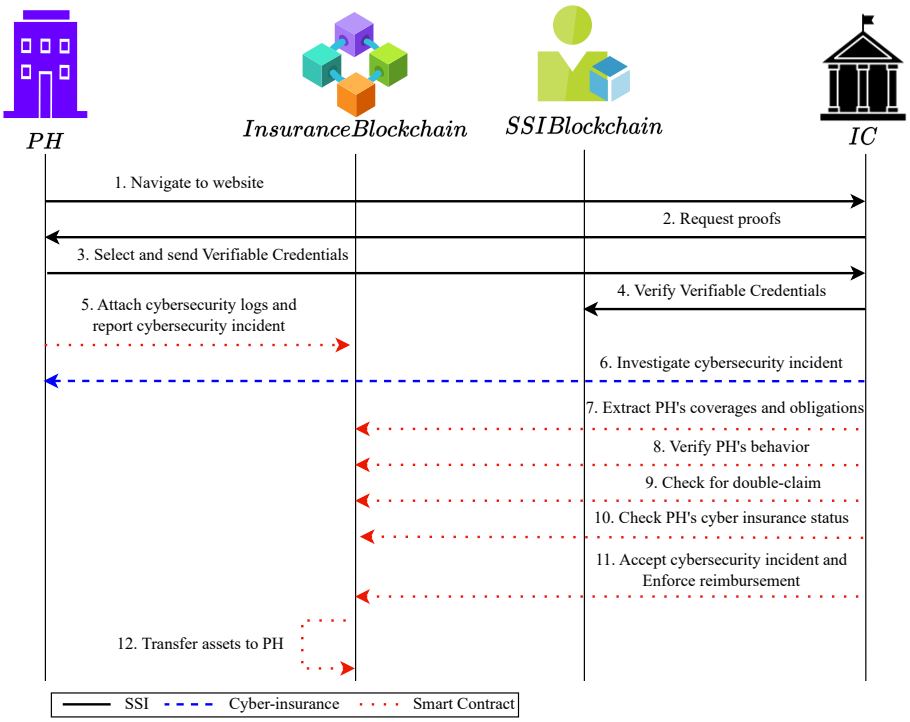

Figure 4: Incident report and reimbursement

gibility for buying a cyber insurance contract. `INCHAIN` substitutes the rigid verification processes that occur on IC's side with automated processes provided by the SSI (`CH2`). Hence, the IC will not allot resources to validate attributes submitted by potential PHs. In addition, it is directly connected with the `CH6`; `INCHAIN` with the SSI integration achieves to equip ICs with a collection of methods that allows them to confirm the identification of their PHs and verify they are acting legally. Moreover, it is well-known that ICs have to store data regarding their PHs becoming targets of cybersecurity attacks (e.g., hackers perform data breaches on ICs to steal PHs' sensitive information). However, with SSI, data is stored on the PHs' side, eliminating many threats related to centralized storage. The information stays in the hands of the PHs, giving the IC permission to view the necessary data. It means that hackers can no longer break into large databases held by ICs to view sensitive data, eliminating many threats for ICs (`CH5`). Also, the gathering of PHs' data eliminates the `CH1` as long as the IC can know important information about its cybersecurity exposure (e.g., security controls, cybersecurity behavior, frequency of cybersecurity incidents). Finally, the collected data during the audits stored within the Insurance Blockchain can be used in the future for underwriting and pricing premium processes for these PHs or future ones.

3.3.3 Incident Report and Reimbursement

During a cyber insurance lifetime, a PH may need to report to its IC a cybersecurity incident having as its ultimate goal to receive reimbursement following their agreement as part of the agreed cyber insurance and the Smart Contract rules. Figure 4 depicts this operation, which is responsible for handling the report of a cybersecurity incident by the PH, the investigation of it by the IC, and the payment order by the latter. It also influences the classic cyber insurance processes entitled *Claims Submission*, *Claims Validation and Auditing*, and *Claims Payment*. First, the process of *Claims Submission* is performed by the PH, which is becoming an automated process due to the Smart Contract functions entitled `IncidentReport`, and `IncidentResponse` (see Sections 2.4 and 3.3.2). Moreover, it substitutes the bureaucracy that characterizes the rigid way of reporting a cybersecurity incident (e.g., email and questionnaires). The same applies to the process named *Claims Payment*. Once an IC accepts the PH's reimbursement, it calls a Smart Contract function and automatically reimburses the PH. In addition, `INCHAIN` enhances the *Claims Validation and Auditing* process with accurate cybersecurity data from the VCs. This data includes new information that has not been considered yet by the existing methods (e.g., employee behavior against phishing attacks). In addition, it becomes more agile

since the Smart Contract function *Check PH Obligations* assists auditors by returning if the PH meets its obligation during the incident period. This opinion comes from the VC's extracted data. It is directly related to the investigation of a cybersecurity incident since the results can be more precise due to the exploitation of the accuracy that characterizes the collected historical data.

For the declaration of a cybersecurity incident (see `Steps 1 - 12` depicted in Figure 4), the PH has to prove its identity to the IC. The IC will request proof from the PH to confirm that it is a legitimate PH with a cyber insurance contract issued by the IC. Let us assume that the PH is the victim of a ransomware attack, with the attackers demanding a ransom of 100K €. While the PH looks within its wallet at the VCs it holds, it can choose to send the entire claim or only a subset of it, ensuring minimal disclosure of its data and proving that it is the legitimate holder of the VCs. Then the IC validates the authenticity of the received VCs by verifying the signatures of the PH's and IC's DID stored within the SSI Blockchain (`Steps 1 - 4`). Once the identification is completed, the PH notifies its IC about the cybersecurity incident (`Step 5`).

The PH provides detailed reports and data that describe the incident (e.g., firewall, IDS, IPS, SOC logs). As a result, the IC performs an incident investigation and, based on the results, decides whether to accept or reject the reimbursement request (`Step 6`). Also, the IC calls Smart Contact functions to extract the PH's obligations that must be met based on its contract and verify that the PH indeed meets them (`Steps 7 - 8`). Last but not least, the IC searches within the Insurance Blockchain to verify that the PH has not submitted the same claim (e.g., recovery expenses from the same ransomware attack) to a different IC (`Step 9`). Then, the IC checks PH's limit of liability and deductible (`Step 10`). The IC checks if the PH has remaining money for its coverages. If the amount is equal to zero, the process is terminated. Otherwise, IC accepts and forces automatic payment to the PH's wallet (`Steps 11 - 12`).IC compensates the PH with 96K €. Then, the limit of liability is automatically reduced to 404K € for the next incident following the reimbursement. However, in the event of a request rejection or identification of double-claim[4], the operation is terminated in `Step 7` or `Step 8` correspondingly. Moreover, in case of Smart Contract's rules violation, the IC triggers a Smart Contract function to decrease PH's reputation.

[4] When a business has insurance cover in respect of the same risk and subject matter from more than one insurer and submits a claim for the same incident to them.

This operation can address the cyber insurance challenges entitled `CH1`, `CH2`, `CH3`, and `CH4`. `INCHAIN` uses Smart Contracts and aims to simplify interactions between a PH and its IC regarding the cybersecurity incident report (`CH2`). In the event of a cybersecurity incident, a PH triggers a Smart Contract function (i.e., the function `IncidentReport`), and automatically its IC gets notified of it. In terms of response, IC can immediately begin incident and forensic investigation. In the end, the IC reimburse the PH by triggering the proper Smart Contract function. Moreover, all incidents with their IDs and attributes stored in the Insurance Blockchain prevent dishonest PHs from reporting the same incident multiple times (`CH3`).

Finally, the use of SSI and VCs deters hackers from stealing PHs' identities by performing masquerade attacks (`CH4`). The VC's claims can be verified only by its owner, which securely stores the correlated private key (see Section 2.4.3). Finally, the IC collects all the cybersecurity data related to the incident and stores it within its Insurance Blockchain to access it later, addressing the challenge `CH1`.

4 Exploring the Value of INCHAIN

This section demonstrates how `INCHAIN` aligns with the established cyber insurance processes outlined in Section 3.1. Furthermore, it effectively addresses the challenges that the cyber insurance landscape poses, as discussed in Section 2.3. Finally, a comparative analysis is conducted with related works, as presented in Section 2.2, to illustrate the uniqueness and effectiveness of `INCHAIN`.

4.1 INCHAIN Capabilities Against Cyber Insurance Processes and Challenges

The `INCHAIN` architecture fulfills all cyber insurance processes outlined in Table 5, with the exception of *Market Research* and *Pricing Premium* (as discussed in Section 3.1). *Market Research* primarily involves communication between a PH and its CIB, and thus falls outside the scope of this work. Similarly, `INCHAIN` does not provide a pricing formula for determining the premium, as this is also beyond the scope of this work.

First and foremost, the `INCHAIN` operation named *Verifiable Credential Issuance* (see Section 3.3.1) as its name implies, is responsible for issuing VCs to a PH. It can be observed that the `INCHAIN` architecture fulfills the cyber insurance process of *Client Registration and Validation* (as discussed in Section 3.1), as the PH is equipped with credentials that contain verified

Table 5: Cyber insurance processes and INCHAIN operations

Cyber Insurance Processes	INCHAIN Operations		
	Verifiable Credential Issuance	Verifiable Credential Verification and Cyber Insurance Issuance	Incident Report and Reimbursement
Client Registration & Validation	✓	✓	✗
Underwriting	✗	✓	✗
Claims Submission	✗	✗	✓
Claims Validation & Auditing	✗	✗	✓
Claims Payment	✗	✗	✓

data from a trustworthy entity (i.e., NCSA). Next, the INCHAIN operation *Verifiable Credential Verification and Cyber Insurance Issuance* as its name implies, includes the verification of a PH's VCs by its IC and upon successful verification the cyber insurance issuance. In particular, VCs automate the *Client Registration and Validation* process. Also, a PH and its IC exchange only accurate data among them, used within the underwriting process. Finally, the *Incident Report and Reimbursement* operation, as its name implies, is responsible for handling claims and includes the *Claims Submission*, *Claims Validation and Auditing*, and *Claims Payment* processes. Its main pillar is the *Smart Contract* functions. On the one hand, the PH triggers the `IncidentReport` function to submit a claim (i.e., *Claims Submission*). On the other hand, other functions (i.e., `IncidentResponse`, `PHObligationChecks`, as well as `AssetTransfer`) are triggered by the IC to initiate investigations and to force the reimbursement.

Table 5 depicts the aforementioned correspondence between the cyber insurance processes (see Section 3.1) and INCHAIN operations (see Section 3.3). The correspondence between cyber insurance processes and the INCHAIN's operations is indicated using the symbols ✓ and ✗. The ✓ symbol signifies that there is a correspondence between a cyber insurance process and an INCHAIN's operation, while the ✗ symbol indicates that there is no such correspondence.

However, INCHAIN can be characterized by the following drawbacks. First, it does not include a formula to calculate the premium of a cyber insurance contract; this process occurs offline at IC's side. Moreover, INCHAIN does not perform an automated incident investigation to decide whether to reimburse an incident; this process also occurs offline. It requires seamless communication between the PH and its IC, including interviews and exchange of logs that need to be analyzed offline by the latter.

In general, it is strongly arguable that INCHAIN can address all cyber insurance challenges mentioned in Section 2. This observation is further extrapolated below.

CH1* – *Lack of Data. INCHAIN utilizes the Blockchain network as a repository to securely store cybersecurity data related to its PHs. As mentioned above (see Section 2.4.1), the Blockchain is an unchangeable, everlasting digital data archive. INCHAIN is equipped with processes that automatically upload records to Blockchain with data related to audits, risk assessment, forensic investigation, and incidents (see Figures 3 and 4). A record stored in the chain cannot be altered, deleted, or otherwise tampered with. Moreover, data accumulates when it cannot be removed. In INCHAIN, an event will be recorded across nodes (e.g., the record of a cybersecurity incident), also known as on-chain data. This enables continuous cybersecurity data gathering related to IC's PHs. The generation of accurate historical data will be a meaningful indicator for cyber insurance processes (*Underwriting* and *Pricing Premium*). Further, the INCHAIN smart contracts incorporate functions capable of retrieving real-time cybersecurity-related information from PHs, such as the frequency of attacks, and securely storing this data within the Blockchain. The adoption of SSI is pivotal in addressing this challenge, ensuring that the involved ICs collect only accurate and up-to-date PH information. This approach eliminates the reliance on outdated or incomplete data stored in centralized databases. As a result, ICs can provide fair premiums tailored to the specific needs of each PH, leveraging statistics derived from the collected historical data. For instance, they can consider data on the most attacked industry and the most common cybersecurity vulnerabilities.

CH2* – *Lack of Automated Tasks. INCHAIN integrates Smart Contracts and SSI to introduce automatically performed tasks. First, by automating cyber insurance claims processes, Smart Contracts can eliminate paperwork and time-consuming processes. The INCHAIN smart contract includes the *Incident Report* function, enabling PH to automatically report cybersecurity incidents to the IC without the need for email communication. Subsequently, depending on the IC's choice to manage the cyber incident internally, the following functions can be invoked: *Contract Analysis*, *PH Obligation Checks*, and *Violation*. In scenarios where the incident response is outsourced to an external firm, the *HandleIncident* function comes into play. Lastly, the

AssetTransfer function automates the payment process for submitted claims. In essence, the functions provided by the smart contract play a crucial role by automating significant aspects of Claims Submission (CIP6), Claims Validation and Auditing (CIP7), and Claims Payment (CIP8). Automating cyber insurance tasks reduces costs significantly; an essential factor for PHs and ICs. Second, SSI enables ICs to perform verification processes automatically (see Section 3.3). `INCHAIN` with SSI substitutes the bureaucracy and labor process of verifying paper documents, contracts, attributes, and IDs. In `INCHAIN`, ICs, via SSI and Blockchain, are reassured that the attributes of a submitted identity are accurate, and they can also immediately check its validator (e.g., NCSA) without contacting it.

CH3 – Fraudulent Claims. It is the first time that a work addresses this challenge (see Table 7). `INCHAIN` eradicates the frequency of fraudulent claims through the integrated SSI approach since the Insurance Blockchain will be accessed only from verified PHs who meet specific requirements. Furthermore, through the Smart Contract implementation, when a claim is submitted for a cybersecurity incident, the IC could check if multiple claims are submitted for the same incident, ensuring that only valid claims are reimbursed. In particular, in case of an incident, the IC can search within the Insurance Blockchain to find similar claims by the subject PH investigating the attached logs. Thus, all fraudulent claims are eradicated. Also, within the Insurance Blockchain, each token is unique and the ledger is immutable without replicable assets (e.g., a cybersecurity incident claim can occur only one time).

CH4 – Identity Theft. ICs face attacks from cyber criminals that are tied back to PHs' for credential theft (e.g., a masquerade attack). `INCHAIN` utilizes SSI and aims to defend its infrastructure from attack vectors targeting data verification (e.g., attackers masquerading as PHs to steal reimbursement). The `INCHAIN` verification system is based on SSI and is used to verify the VCs and ensure that the content interactions match the role of the issuer (such as NCSA), preventing collaboration with fake issuers. In addition, the constantly updated SSI Blockchain provides validated issuer information to ICs. Thus, ICs can determine the validity of both the issuer (e.g., NCSA) and the VC when it is submitted to their service. A VC signed by its issuer is stored within a digital identity wallet (see Section 2.4.3). Thus, the data contained within it and shared with ICs cannot be changed without being flagged (e.g., as an error) by the original issuer. In essence, only the original issuer can alter a VC's data. In addition, the digital identity wallet remains encrypted at rest as well as in motion. Without the keys (see Section 2.4.3) to this encrypted wallet, the data is not accessible outside of it.

CH5 – Loss of Sensitive Data. Centralized verification systems make organizations vulnerable to large-scale hacks and data breaches (e.g., a data breach in Marriott hotels [77]). `INCHAIN` aims to prevent this kind of attack in ICs using SSI. Generally speaking, SSI safeguards privacy by removing the need to store personal information on a central database and gives individuals greater control over what information they share. Through VCs, SSI lets PHs control what they disclose with ICs [76] (i.e., selective disclosure) avoiding centralized data storage. PHs are SSI identity holders and control their own VCs. These VCs are kept locally on a PH's digital identity wallet and digitally signed with its private key and the NCSA keys (see Section 2.4.3), ensuring its ownership. ICs receive VCs safely to provide a service. Thus, the PH retains control of its data and only grants the IC access to the information it requires. As a result, there is far less risk of harm to the IC, as attackers will no longer be able to compromise the IC's database and steal sensitive data. Apart from protecting the ICs, SSI also protects PHs from fraudulent ICs through secure authentication, selective disclosure of information, decentralized verification networks, reputation and trust models, an immutable audit trail, privacy-preserving protocols, and community governance. SSI utilizing cryptographic techniques for secure authentication allows PHs to prove their identity without revealing unnecessary personal information. PHs have control over the information they share, reducing the risk of exposing sensitive data to fraudulent ICs. In addition, SSI's decentralized verification networks and reputation models ensure that trusted entities vouch for authenticity, and users can assess verifiers' trustworthiness through ratings and reviews. The immutable audit trail enables accountability and identification of fraudulent ICs, while privacy-preserving protocols minimize data exposure.

CH6 – Know Your Customer. Another aspect of the proposed architecture is the *Know Your Customer* approach to completion. In `INCHAIN`, the SSI is responsible for the identification of PHs, as the data associated with a PH's identity is stored, shared, and used for verification on distributed ledger technology. The use of VC on SSI enhances the security level of identification as the VC is cryptographically constructed to prove its issuer, owner, and validity. Additionally, the VC claims are not tampered with. On the other hand, the Insurance Blockchain (see Figure 1) is responsible for continuously monitoring PHs during a cyber insurance contract. Overall, SSI and the Insurance Blockchain help

Table 6: Cyber insurance challenges and Candidate Technologies

Cyber Insurance Challenges	Candidate Technologies		
	Blockchain	Smart Contracts	SSI
CH1 – Lack of Data	✓	✓	✓
CH2 – Lack of Automated Tasks	✗	✓	✓
CH3 – Fraudulent Claims	✗	✓	✓
CH4 – Identity Theft	✗	✗	✓
CH5 – Loss of Sensitive Data	✓	✗	✓
CH6 – Know Your Customer	✗	✗	✓
CH7 – Information Asymmetry	✗	✓	✗

to reduce costs by decreasing the need for personnel focused on *Know Your Customer* tasks, enhancing the security of identification, shortening processing time, and improving the PHs experience.

CH7 – Information Asymmetry. `INCHAIN` eliminates the information asymmetry between the ICs and PHs regarding the cyber insurance contract misunderstanding. In particular, the `INCHAIN` Smart Contract (see Section 3.3.2) is equipped with a specific function (i.e., `ContractAnalysis`). The Smart Contract, which is a digital representation of the cyber insurance contract, includes the definitions of each covered incident. For instance, if the PHs raise the following question: *"What does the insurance cover regarding a cyber-extortion threat?"*, the Smart Contract function `ContractAnalysis` will respond not only with its definition but the circumstances that should be met in order to be covered. Thus, with `INCHAIN`, the PHs will be deterred from decreasing their security investments after obtaining cyber insurance. Moreover, `INCHAIN` contributes significantly to the underwriting process of cyber insurance. In particular, the `INCHAIN` Smart Contract (see Section 3.3.2) is equipped with a specific function (i.e., `PH Obligation Checks`) that checks if the installed cybersecurity controls of PH comply with its cyber security contract obligations. This feature of INCHAIN could save the underwriter a significant amount of time that he would have spent with the traditional way of interviewing policyholders and then editing their responses to determine if they are consistent with the policyholder's obligations. What INCHAIN cannot eliminate, however, is the human critical thinking of the underwriter who will make the final underwriting decision. Last but not least, `INCHAIN` via function Incident Response checks if the requested indemnification of PH in Claims Submission (CIP6) can be served by the attribute maximum indemnity limit (or `INCHAIN`'s attribute named Limit of Liability 3.3.2). The value of Limit of Liability is defined in `INCHAIN` when it is called the function PH Creation.

Table 6 describes the cyber insurance challenges being addressed by the `INCHAIN` candidate technologies. First and foremost, Blockchain contributes to mitigating *CH1 – Lack of Data* and *CH5 – Loss of Sensitive Data* since it provides an immutable and secured data storage at the IC's side and transparency for each related transaction. Next, the integration of Smart Contracts assists in the mitigation of the *CH1 – Lack of Data*, *CH2 – Lack of Automated Tasks*, *CH3 – Fraudulent Claims*, and *CH7 – Information Asymmetry*, since these are equipped with functions (see also Section 3.3) to perform the required actions for gathering real-time cybersecurity-related PHs' data, to automatically execute processes for incident report and handling, as well as, to assist PHs to understand their obligations against their contract. While SSI commits to mitigating *CH1 – Lack of Data*, *CH2 – Lack of Automated Tasks*, *CH3 – Fraudulent Claims*, *CH4 – Identity Theft*, *CH5 – Loss of Sensitive Data*, and *CH6 – Know Your Customer*. This occurs because SSI can allow ICs to gather not only updated but also the minimum required PH's data to perform cyber insurance processes (see also Section 3.1) and provide full identity control on the involved PHs. Overall, we can observe that `INCHAIN` aims to face the cyber insurance challenges (see also Section 2.3), combining features from more than one candidate technology and merely exploiting Blockchain features to develop applications for enhancing existing cyber insurance processes.

4.2 Comparative Analysis of Related Works and INCHAIN in Addressing Cyber Insurance Challenges

Table 7 compares related works (see Section 2.2) with `INCHAIN` against the cyber insurance challenges (see Section 2.3); the comparison is based on the following signs: ✓, ✗, ✦. The ✓ sign shows that the respective challenges consist of an advantage of the method over the others, in the sense that the work addresses the challenge. The ✗ sign shows that the challenge is considered a deficiency of the work, in the sense that the challenge is not addressed. When the ✦ sign is displayed, it means that the respective work does not include all the details needed, and assumptions were needed to come to a conclusion. Here, we answer the fourth research question (*RQ4 – How does the literature address the existing challenges of cyber insurance with Blockchain and smart contracts?*). The selection of works for comparison with `INCHAIN` was based on the following criteria:

1. The work exclusively lies in the cyber insurance field.
2. The work utilizes at least one of the candidate technologies (see Section 2.4).

Table 7: Cyber insurance challenges fulfillment of related work

Challenges	Works					
	Franco et al. [10]	Lepoint et al. [11]	Vakilinia et al. [12]	Xu et al. [13]	Farao et al. [14]	INCHAIN
CH1 - Lack of Data	✗	✓	✗	✗	✓	✓
CH2 - Lack of Automated Tasks	✓	✓	✓	✓	✓	✓
CH3 - Fraudulent Claims	✗	✗	✗	✗	✗	✓
CH4 - Identity Theft	✗	✦	✗	✗	✗	✓
CH5 - Loss of Sensitive Data	✗	✦	✗	✗	✗	✓
CH6 - Know Your Customer	✗	✗	✗	✗	✗	✓
CH7 - Information Asymmetry	✗	✗	✗	✗	✓	✓

3. The work aims to address cyber insurance challenges (see Section 2.3).

Franco et al. [10] propose SaCI on top of Ethereum, utilizing Smart Contracts. SaCI uses Smart Contracts to automate the processes of premium payment, contract updates, claim requests, dispute resolutions, and check of contract information and its integrity. Thus, SaCI addresses the challenge CH2. However, because of Ethereum, each Smart Contract function has a gas fee. On the one hand, this can limit the number of claims submitted by a PH, forcing it to submit claims only for real incidents. On the other hand, in case of identity theft, the attacker can overcharge and waste the accumulated money of the limit of liability. Thus, a PH may be unable to submit a claim for a real incident because there will not be enough money in its wallet for spending. Also, this system lacks a verification method to check the PH's legitimacy before submitting a claim request. The authors do not analyze how ICs verify the PHs' attributes. Furthermore, the authors do not consider collecting cybersecurity data for use in future cyber insurance processes. Overall, SaCI does not address CH1, CH3, CH4, CH5, CH6, and CH7.

Lepoint et al. [11] present BlockCIS on top of Hyperledger Fabric, utilizing Smart Contracts. BlockCIS leverages the automated nature of smart contracts (on the IC side) but is entirely decoupled from the payment aspect of the blockchain (contrary to INCHAIN). BlockCIS is a continuous monitoring and processing cyber insurance system focusing on the confidentiality and privacy of the collected and stored data within the system. ICs use Smart Contracts to devise premiums tailored to a PHs's security posture, and the latter can prove that its cyber insurance covers a potential cyber incident. In addition, BlockCIS includes access control rules to limit access to its data. It is assumed that based on the implemented access control rules, BlockCIS may defend against cyberattacks related to identity theft and loss of sensitive data. However, we cannot conclude with 100% confidence because the respective work does not include all the necessary implementation details. Thus, it is assumed that BlockCIS addresses CH1 and CH2 challenges, while the CH4 and CH5 are addressed under implementation assumptions. However, the authors do not consider a method to verify that PHs submit accurate data nor to monitor any change in its infrastructure. Finally, BlockCIS does not include a method to prevent fraudulent claims and eliminate information asymmetry. Thus, BlockCIS does not address the CH3, CH6, and CH7 challenges.

Vakilinia et al. [12] and Xu et al. [13] propose cyber insurance crowdfunding frameworks on top of the Ethereum network. Smart Contracts can perform crowdfunding initialization, bidding, wrapping, and reimbursement actions. Thus, both works address the CH2 challenge. However, the proposed frameworks lack a method to collect cybersecurity data for future cyber insurance use and to prevent fraudulent claims. Moreover, the frameworks are not equipped with security measures to prevent cybersecurity attacks related to identity theft and loss of sensitive data. Thus, in case of identity theft, the attacker can overcharge and waste the PH's accumulated money of the limit of liability. Hence, a PH may not submit a claim for a real incident because there will not be money in its wallet for spending. Furthermore, the authors do not analyze the method that ICs follow to verify a PH's attributes, do not consider a method to be updated for changes in PHs's infrastructures, and do not include a method to eliminate the information asymmetry. Consequently, both works do not address CH1, CH3, CH4, CH5, CH6 and CH7.

Finally, the SECONDO project [14] has been built on top of Hyperledger Fabric. Its Smart Contracts perform actions related to reporting and responding to an incident as well as to forcing reimbursement. Thus, Farao et al. [14] can address the CH2 challenge. Moreover, SECONDO is equipped with a continuous risk monitoring tool that collects PHs' cybersecurity data and stores it within the Blockchain. The data is used for future cyber insurance processes (i.e., underwriting). Thus, SECONDO addresses the CH1 challenge. Moreover, it includes a cyber insurance policy ontology that eliminates the information asymmetry between the PHs and ICs, addressing the CH7 challenge. However, SECONDO does not have a mechanism in place to prevent eligible PHs from submitting fraudulent claims or to verify the PH's eligi-

bility before the claim submission. Finally, it does not consider a method to gather only accurate PHs data during each cyber insurance process. Overall, SECONDO cannot address the CH3, CH4, CH5 and CH6 challenges.

Overall, the previous analysis raises the following observations. First and foremost, all related works address the challenge CH2 using Smart Contracts. INCHAIN addresses it via the Smart Contracts integration. Next, [11,14] and INCHAIN address challenge C1. These works utilize their Blockchain implementation to store cybersecurity data for future cybersecurity use. Furthermore, the literature [10–14] does not address the challenge CH3 regardless of its importance. However, in INCHAIN, ICs search within the Insurance Blockchain to find similar claims by the subject PHs investigating the attached logs. [11] and INCHAIN address the challenge CH4. The other works do not implement a method to protect their system from this since a PH can use the network certificate to trigger a Smart Contract function. Thus, if attacks steal the credential, they can call any Smart Contract function without limitations. The authors in [11] allow the Smart Contract use based on access control rules to prevent PHs' identity stealing. However, in INCHAIN, a PH has to be authorized via VC verification before submitting a claim. It occurs with VCs stored in secured digital identity wallets. Therefore, INCHAIN depends on the fact that VCs can be accessed only by their eligible holders. It is the one knowing the key pair to access the digital identity wallet and to use its VCs.

In addition, [11] and INCHAIN address the challenge CH5. The works [10, 12, 13] do not include any method to protect data since they do not collect them. However, [11, 14] collect cybersecurity data. The authors in [14] depend on the certificates issued by the Blockchain. Thus, a node with the correct certificate can perform actions to the collected cybersecurity data without limitation. However, the work [11] limits access to the collected data via an access control policy. In contrast, INCHAIN uses VCs to allow access to its collected cybersecurity data stored within the Insurance Blockchain. Further, challenge CH6 has been addressed only by INCHAIN. It includes SSI to collect accurate data regarding PHs's behavior and assets. Finally, [14] and INCHAIN solve the challenge CH7. On the one hand, Farao et al. [14] include a cyber insurance policy ontology that analyzes each contract isolating its coverages and exclusions. On the other hand, INCHAIN uses a Smart Contract function that can be triggered anytime by the PHs and the ICs. It is responsible for defining the cybersecurity threats covered for PHs and outlining the obligations they must fulfill in order to be eligible for reimbursement.

5 Discussion

This section presents an analysis of the risks inherited by the integration of Blockchain and SSI, the presentation of well-know and open-source Blockchain platforms and SSI implementation that could be leveraged by the cyber insurance ecosystem, an analysis of INCHAIN limitation, along with suggestions for future research and development avenues that can be pursued to enhance its capabilities and expand its impact.

5.1 Inherited Risks of Blockchain and SSI Integration

Now, we analyze the risks inherited to the cyber insurance ecosystem integrating Blockchain and SSI. While Blockchain technology inherits numerous advantages and opportunities, it also poses certain risks in the context of cyber insurance. Below, we highlight the risks associated with the use of blockchain in cyber insurance:

Smart Contract Vulnerabilities: Smart contracts, which are self-executing agreements on the blockchain, contain vulnerabilities [78] that attackers can exploit. Bugs or coding errors in smart contracts could lead to unintended consequences or allow unauthorized access to sensitive information. However, a contingency plan includes testing protocols consisting of penetration tests and audits leading to the identification of Smart Contracts' vulnerabilities and their address.

Data Privacy and Security: Blockchain is touted for its security; however, it is not immune to cybersecurity attacks [79]. While the decentralized nature of blockchain can make it more difficult to tamper with data, it does not guarantee absolute security. For instance, if the private keys used to access blockchain-based systems are compromised, it could lead to unauthorized access, data leaks, or loss of funds. However, a contingency plan may include actions related to secure storage for keys and certificates, as well as the implementation of robust encryption mechanisms (e.g., AES algorithm).

Oracles and External Data Sources: Blockchain-based insurance platforms often rely on oracles to obtain external data, such as information about security breaches or PHs claims [80]. However, the accuracy and reliability of these external data sources can be a concern. If the oracles are compromised or provide inaccurate information, it can undermine the integrity of the insurance claims process. Thus, a contingency plan may include mechanisms for validating and verifying data accuracy obtained from oracles and external data sources.

Lack of Standardization and Regulations: The blockchain is still in its infancy; thus, the lack of standardized protocols and interoperability between different blockchain platforms can hinder blockchain's scalability and widespread adoption in the insurance industry. Therefore, ICs may face challenges integrating blockchain-based solutions with their existing systems, leading to inefficiencies or compatibility issues. Yet, a contingency plan may include the development of flexible and modular blockchain solutions that can adapt to future changes and advancements in the blockchain.

Moreover, the integration of SSI inherits risks to the cyber insurance ecosystem, these are elaborated below:

Social Engineering and Manipulation: SSI systems rely heavily on user consent and identity control. However, within the cyber insurance ecosystem, this can make PHs more susceptible to social engineering attacks or manipulative practices, where they may unknowingly grant access to their identity information to malicious actors pretending to be their IC. This can lead to unauthorized access to sensitive data and misuse of identity information. Nonetheless, a contingency plan may include actions for educating PHs to detect and avoid phishing attacks, fraudulent requests for identity information, and unauthorized access attempts building and promoting the human firewall approach.

Increased Risk of Identity Theft: SSI systems store sensitive data on distributed ledgers, and the security of these systems becomes critical. If vulnerabilities exist in the SSI infrastructure or malicious actors gain unauthorized access, it could lead to widespread identity theft and fraud. Such incidents could result in a surge in fraudulent claims and financial losses for ICs. A contingency plan may include the utilization of security enclaves, robust access control mechanisms, as well as encryption of data in rest and in transit.

System Availability: The risk of a single point of failure is an important consideration when implementing SSI systems. Such a system failure may disrupt and interrupt the availability and functionality of the system, making it inaccessible to legitimate users. However, a contingency plan may include actions related to robust infrastructure design, traffic monitoring, and anomaly detection.

5.2 Blockchain Platforms and SSI Implementations Suitable for the Cyber Insurance Ecosystem

Now, we present well-known and open-source blockchain platforms (i.e., Hyperledger Fabric, Ethereum) and SSI implementations (uPort, Hyperledger Aries) that could be used for cyber insurance.

Hyperledger Fabric is an open-source blockchain platform that enables organizations to construct and administer their own distributed ledger systems. It provides the required tools and frameworks for constructing blockchain-based insurance applications with features such as smart contracts, privacy, and authorized access. The strongest feature of Hyperledger Fabric is the execution of smart contracts. ICs can automate policy issuance, claims processing, and premium calculation processes using smart contracts. Moreover, Hyperledger Fabric enables the construction of private channels in which only a select group of participants can access the shared data. This enables ICs to share sensitive information, such as policy details and claims data, with relevant parties in a secure manner while maintaining data privacy and confidentiality. Finally, Hyperledger Fabric supports pluggable consensus mechanisms, enabling ICs to select the most appropriate consensus algorithm for their particular requirements in cases such as policy revisions, claim settlements, and other crucial network decisions.

Ethereum is a decentralized, open-source blockchain infrastructure that allows the creation of smart contracts and decentralized applications (DApps). On Ethereum, numerous insurance-related DApps have been developed, offering solutions for areas such as parametric insurance, claims processing, and peer-to-peer insurance. The most crucial feature of Ethereum that can be utilized for cyber insurance purposes is its support for smart contracts. Cyber insurance policies can be implemented on the Ethereum blockchain as smart contracts. Smart contracts automate policy issuance, premium calculation, claims processing, and payout calculations based on predetermined cyber insurance requirements, reducing documentation and administrative costs. Moreover, Ethereum can support asset tokenization, representing a fraction of ownership in the underlying asset. More particularly, a series of token standards have developed to support asset tokenization of Ethereum (i.e., ERC-20, ERC-721, ERC-777, ERC-1155, ERC-4626) [81]. Another unique concept of Ethereum is gas consumption, which refers to the quantity of computational work required to execute a transaction or smart contract. Gas is a fee mechanism to prevent spam and fairly allocate network resources. Spammers would have to pay substantial gas fees to submit a high volume of spam transactions. This economic cost renders spamming economically unviable for most attackers, as they would be required to incur expenses without obtaining a significant advantage. Finally, oracles enable Ethereum to integrate with exter-

nal data sources collecting data from them and providing it to Ethereum smart contracts. A prime example of oracles utilization is that oracles can provide data feeds pertaining to top vulnerabilities, percentages of cyber-attacks, or other pertinent information, enabling parametric cyber insurance and claim settlement procedures.

uPort is a platform for DID constructed on the Ethereum blockchain and developed by ConsenSys. It can enable users to establish self-governing identities and manage their digital credentials. ICs can use uPort to validate the identities of PHs, reducing the risk of identity fraud and building trust between parties. Moreover, uPort can be used to store and present cyber insurance documentation. Instead of keeping cyber insurance paper documents, PHs can retain their cyber insurance policies in their uPort wallets as digital credentials, simplifying the proof of coverage, reducing paperwork, and enhancing efficiency. Also, having all their claims-related documents (e.g., cyber-attack accident reports) in VCs, PHs can selectively share these documents with ICs, ensuring privacy and control over sensitive data. Lastly, the compatibility of uPort with other decentralized identity systems and platforms can permit the exchange of VCs across networks and ecosystems, enhancing the integration of ICs with existing systems and processes.

Hyperledger Aries is an open-source initiative under the Hyperledger umbrella of the Linux Foundation. It is a framework for developing solutions for DID and interoperable identity systems, and it offers a set of tools, libraries, and reusable components that facilitate the exchange of verifiable credentials and the creation of SSI applications. Hyperledger Aries can enable ICs to establish and authenticate the digital identities of the cyber insurance ecosystem's stakeholders, thereby augmenting the integrity and safety of the cyber insurance process. The VCs can be stored in a PHs' secure storage location named Hyperledger Aries wallet. Beyond the role of VCs in the authentication of digital identities, the content of VCs can be related to PH's cyber incidents, such as cyber incident reports or forensic data. This information can be selectively shared with other parties involved in the claims process through the feature of Hyperledger Aries named Selective Disclosure, thereby securely facilitating the exchange of claim-related information and reducing paperwork. Finally, Hyperledger Aries uses secure messaging protocols and cryptographic mechanisms, since it is based on Hyperledger Ursa [82], to safeguard the confidentiality and integrity of communications.

5.3 Limitations

Foremost among the limitations of `INCHAIN` is the absence of a comprehensive module for identifying cyber insurance contracts on the web, making it difficult for PHs to locate the appropriate policy for their needs. Without a simple way to compare contracts from multiple ICs, PHs either struggle to comprehend the terms and conditions of each insurance, or they may overlook critical coverage alternatives that might protect them against cyber attacks. The reason that `INCHAIN` does not deliver such a formula is because of the absence of a crawler to scrap not only the web but also ICs' websites to identify their policies and analyze them at the same time. Thus, in `INCHAIN`, PHs need to work closely with CIBs to find the right policy for their needs.

On top of the aforementioned limitation, `INCHAIN` lacks a well-defined mechanism for calculating cyber insurance premiums. This represents a significant impediment for both ICs seeking to assess risk accurately and potential PHs who require transparent and reliable pricing information. Effective risk assessment is a critical challenge for ICs operating within the `INCHAIN` ecosystem. However, without a precise method for calculating the premium, navigating the complex landscape of potential PHs with varying levels of risk becomes even more challenging. This presents a significant obstacle to accurately assessing PHs' risk levels and underscores the need for enhanced risk modeling capabilities, leading to coverage overcharging or undercharging. Thus, in `INCHAIN`, ICs struggle to evaluate premium, while PHs find it challenging to determine which ICs offer the greatest value. The cyber insurance premium is influenced by vast parameters including but not limited to the PH's number of employees, its base rate, and the accepted downtime. The reason for the absence of the `INCHAIN` cyber insurance premium calculation formula reflects the complexity and constantly changing nature of cybersecurity risks, as well as the need for ICs to tailor their coverage and pricing to the unique needs of each client.

Moreover, `INCHAIN`, via the use of its candidate technologies, aims to increase the volume of cybersecurity-related data (***CH1***). It is observed that collecting vast amounts of data does not guarantee meaningful insights for cyber insurance. New challenges will emerge related to data quality, relevance, and context. Thus, `INCHAIN` will not eliminate this lack of historical data; however, it aims to play an essential role in creating a fertile surface for application and collaboration development for gathering accurate cybersecurity data that can be used in the future regardless of the period's technological state-of-the-art.

It is observed that SSI, due to its characteristics (i.e., decentralized data storage, cryptographic security, selective disclosure, user control, immutable audit trail), enhances the protection of ICs against data breaches and the loss of sensitive data (***CH5***). Since it establishes a more secure and privacy-preserving environment for exchanging and managing gathered sensitive information, reducing the potential risks associated with traditional centralized data storage and handling practices. However, the INCHAIN does not protect the involved PHs from being targeted by fraudulent entities that aim to steal their sensitive data pretending to be trustworthy ICs. This is a crucial issue directly related to the human firewall approach. Thus, PHs should create a contingency plan, including cybersecurity awareness training to learn how to avoid cybersecurity attacks (e.g., phishing attempts).

Smart Contracts through predefined rules enhance the elimination of Information Asymmetry (***CH7***). The INCHAIN's effort via the developed functions of Smart Contract has contributed significantly to the misunderstanding of cyber insurance contracts and the improvement of the underwriting process. However, INCHAIN has not managed to disappear human intervention in underwriting. Human criticism and thinking are indispensable mainly to making final decisions in the underwriting process of cyber insurance.

5.4 Future Work

The research results presented in this paper have the potential to be extended in various ways through future work. First, the proposed cyber insurance architecture can be further analyzed from a functionality and architectural point of view. Use cases and scenarios showcasing the proposed architecture's beneficial aspects can be analyzed in-depth to emphasize the novelty and its relevance to ICs and PHs. Moreover, part of future work is the development of this ecosystem by integrating well-known and robust implementations having the Hyperledger as the main part of the system. In particular, it is a high priority to equip INCHAIN with asset transferring Blockchain application to operate the automated reimbursement from an IC to a specific PH, utilizing the IPFS approach [83] to achieve secure data storage and sharing in a distributed file system, and integrate Aries [84] as an SSI implementation. Cyber insurance professionals should assess the implementation against time consumption and resource depletion.

INCHAIN can also be armed with a formula to calculate the premium of a cyber insurance contract considering parameters such as the total number of security breaches and PHs' reimbursement history. In addition, INCHAIN can be equipped with a cyber insurance policy ontology being responsible to find policies of well-known ICs and analyze them distinguishing their coverage and exclusions. Finally, INCHAIN Smart Contracts can be enriched with a new function responsible for performing automated incident investigation and deciding whether to reimburse an incident.

As cybersecurity attacks become increasingly sophisticated and unpredictable, the demand for cyber insurance contracts is expected to increase over time. Cyber insurance offers a means to transfer risks to a third party. However, there are challenges that need to be addressed in order for the cyber insurance market to grow. The research outcomes presented in this paper serve as a precursor to designing cyber insurance schemes and applications that can effectively address the challenges of the growing cyber insurance market.

6 Conclusion

This paper introduces a novel cyber insurance architecture, INCHAIN, which combines existing technologies such as Blockchain, Smart Contracts, and Self-Sovereign Identity (SSI) to address the challenges of cyber insurance. The proposed architecture is centered around Blockchain, which serves as a fundamental building block, providing security, fairness, trust, and interoperability among the participating entities. Smart Contracts automate the critical tasks of claim handling and payment in the event of a cybersecurity incident. The integration of SSI enables data minimization, robust identification, data interoperability, portability, controllability, decentralization, and transaction transparency, empowering stakeholders to increase their trustworthiness. The proposed ecosystem successfully meets the basic cyber insurance processes and addresses cyber insurance challenges by leveraging the aforementioned technologies, as demonstrated through testing in various scenarios.

In a nutshell, this paper presents INCHAIN as a novel cyber insurance architecture that offers advantages over existing methods. By conducting a comprehensive survey of previous works and comparing them with our proposed architecture, we prove its effectiveness and potential to enhance the cyber insurance industry under a theoretical perspective. The research outcomes presented in this paper not only establish a foundation for the development of cyber insurance schemes and applications but also pave the way for addressing the challenges facing the growing cyber insurance market.

Acknowledgements

This research has received funding from European Commission's Horizon Europe and Horizon 2020 research and innovation programs under grant agreements No. 823997 (SECONDO), No. 101095634 (ENTRUST), No. 101092702 (OASEES), and No. 101070214 (TRUSTEE).

Declarations

Compliance with Ethical Standards.
This article does not contain any studies with human participants or animals performed by any of the authors.

Competing Interests.
The authors declare no conflict of interest.

Research Data Policy and Data Availability.
All data used during this study are included in this published article.

References

1. W. E. Forum, "The global risks report 2022, 17th edition.."
2. R. Böhme, G. Schwartz, *et al.*, "Modeling cyber-insurance: towards a unifying framework.," in *WEIS*, 2010.
3. S. Panda, A. Farao, E. Panaousis, and C. Xenakis, "Cyber-insurance: Past, present and future," in *Encyclopedia of Cryptography, Security and Privacy*, pp. 1–4, Springer, 2021.
4. PANASEER, "2022 cyber insurance market trends report.."
5. Sophos News, "Cyber insurance: there's bad news and there's good news.." `https://bit.ly/3YQBqmP`. Online; Last Accessed: 07/2023.
6. NEW AMERICAS, "Are state-sponsored cyber attacks covered by your insurance?." `https://bit.ly/42g0pTa`. Online; Last Accessed: 07/2023.
7. K. S. Wan, "NotPetya, Not Warfare: Rethinking the Insurance War Exclusion in the Context of International Cyberattacks," *Wash. L. Rev.*, vol. 95, p. 1595, 2020.
8. LLOYD'S, "Shen attack: Cyber risk in asia pacific ports.."
9. LOCKTON, "The cyber insurance dilemma - investment in cyber insurance vs further investment in cyber security.."
10. M. Franco, N. Berni, E. Scheid, C. Killer, B. Rodrigues, and B. Stiller, "Saci: A blockchain-based cyber insurance approach for the deployment and management of a contract coverage," in *Economics of Grids, Clouds, Systems, and Services: 18th International Conference, GECON 2021, Virtual Event, September 21–23, 2021, Proceedings 18*, pp. 79–92, Springer, 2021.
11. T. Lepoint, G. Ciocarlie, and K. Eldefrawy, "Blockcis—a blockchain-based cyber insurance system," in *2018 IEEE International Conference on Cloud Engineering (IC2E)*, pp. 378–384, IEEE, 2018.
12. I. Vakilinia, S. Badsha, and S. Sengupta, "Crowdfunding the insurance of a cyber-product using blockchain," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 964–970, IEEE, 2018.
13. J. Xu, Y. Wu, X. Luo, and D. Yang, "Improving the efficiency of blockchain applications with smart contract based cyber-insurance," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, IEEE, 2020.
14. A. Farao, S. Panda, S. A. Menesidou, E. Veliou, N. Episkopos, G. Kalatzantonakis, F. Mohammadi, N. Georgopoulos, M. Sirivianos, N. Salamanos, *et al.*, "Secondo: A platform for cybersecurity investments and cyber insurance decisions," in *International Conference on Trust and Privacy in Digital Business*, pp. 65–74, Springer, 2020.
15. I. Kalderemidis, A. Farao, P. Bountakas, S. Panda, and C. Xenakis, "Gtm: Game theoretic methodology for optimal cybersecurity defending strategies and investments," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–9, 2022.
16. M. Charalambous, A. Farao, G. Kalantzantonakis, P. Kanakakis, N. Salamanos, E. Kotsifakos, and E. Froudakis, "Analyzing coverages of cyber insurance policies using ontology," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–7, 2022.
17. F. Loukil, K. Boukadi, R. Hussain, and M. Abed, "Ciosy: A collaborative blockchain-based insurance system," *Electronics*, vol. 10, no. 11, p. 1343, 2021.
18. S. Kumar, U. Dohare, O. Kaiwartya, *et al.*, "Flame: Trusted fire brigade service and insurance claim system using blockchain for enterprises," *IEEE Transactions on Industrial Informatics*, 2022.
19. A. S. Yadav, V. Charles, D. K. Pandey, S. Gupta, T. Gherman, and D. S. Kushwaha, "Blockchain-based secure privacy-preserving vehicle accident and insurance registration," *Expert Systems with Applications*, p. 120651, 2023.
20. A. Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "Chainsure: Agent free insurance system using blockchain for healthcare 4.0," *Intelligent Systems with Applications*, vol. 17, p. 200177, 2023.
21. P. Bountakas, C. Ntantogian, and C. Xenakis, "Eknad: Exploit kits' network activity detection," *Future Generation Computer Systems*, vol. 134, pp. 219–235, 2022.
22. S. Dambra, L. Bilge, and D. Balzarotti, "Sok: Cyber insurance–technical challenges and a system security roadmap," in *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 1367–1383, IEEE, 2020.
23. S. Panda, D. W. Woods, A. Laszka, A. Fielder, and E. Panaousis, "Post-incident audits on cyber insurance discounts," *Computers & Security*, vol. 87, p. 101593, 2019.
24. A. Tsohou, V. Diamantopoulou, S. Gritzalis, and C. Lambrinoudakis, "Cyber insurance: state of the art, trends and future directions," *International Journal of Information Security*, pp. 1–12, 2023.
25. Insurance Fraud Bureau New Zealand Sophos News, "Claiming with multiple insurers.." `https://bit.ly/42bkhHc`. Online; Last Accessed: 07/2023.
26. ENISA, "Identity theft: ENISA Threat Landscape."
27. G. Suciu, A. Farao, G. Bernardinetti, I. Palamà, M.-A. Sachian, A. Vulpe, M.-C. Vochin, P. Muresan, M. Bampatsikos, A. Muñoz, *et al.*, "Samgrid: Security authorization and monitoring module based on sealedgrid platform," *Sensors*, vol. 22, no. 17, p. 6527, 2022.
28. InsurTech, "5 cybersecurity threats hitting insurance companies in 2022.." `https://bit.ly/3TeDhAA`. Online; Last Accessed: 07/2023.
29. SCMedia, "Insurance companies increasingly fall prey to cyberattacks.." `https://bit.ly/3Tl8TEO`. Online; Last Accessed: 07/2023.
30. PWC, "Blockchain, a catalyst for new approaches in insurance.."

31. ZYEN, "Interexchainz research project." `https://bit.ly/3mVDr3T`. Online; Last Accessed: 07/2023.
32. K. Ruan, *Digital asset valuation and cyber risk measurement: Principles of cybernomics*. Academic Press, 2019.
33. A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Computer Science Review*, vol. 24, pp. 35–61, 2017.
34. R. P. Majuca, W. Yurcik, and J. P. Kesan, "The evolution of cyberinsurance," *arXiv preprint cs/0601020*, 2006.
35. S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz002, 2019.
36. R. Böhme and G. Kataria, "Models and measures for correlation in cyber-insurance.," in *WEIS*, vol. 2, p. 3, 2006.
37. R. Böhme, "Cyber-insurance revisited.," in *Weis*, 2005.
38. B. Aziz *et al.*, "A systematic literature review of cyber insurance challenges," in *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 357–363, IEEE, 2020.
39. I. Bashir, *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt Publishing Ltd, 2020.
40. D. Mahmudnia, M. Arashpour, and R. Yang, "Blockchain in construction management: Applications, advantages and limitations," *Automation in Construction*, vol. 140, p. 104379, 2022.
41. Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.
42. A. Sarma, "Smart contracts: A way to modern digital world," in *Blockchain and Deep Learning: Future Trends and Enabling Technologies*, pp. 67–106, Springer, 2022.
43. V. Bolgouras, A. Angelogianni, I. Politis, and C. Xenakis, "Trusted and secure self-sovereign identity framework," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–6, 2022.
44. A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.
45. World Wide Web Consortium (W3C), "Verifiable credentials data model v1.1." `https://bit.ly/3Lqde7M`. Online; Last Accessed: 07/2023.
46. N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 90–95, IEEE, 2020.
47. A. Farao, E. Veroni, C. Ntantogian, and C. Xenakis, "P4g2go: A privacy-preserving scheme for roaming energy consumers of the smart grid-to-go," *Sensors*, vol. 21, no. 8, p. 2686, 2021.
48. A. Muñoz, A. Farao, J. R. C. Correia, and C. Xenakis, "Ic-itpm: integrity validation of software in iterative continuous integration through the use of trusted platform module (tpm)," in *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25*, pp. 147–165, Springer, 2020.
49. A. Muñoz, A. Farao, J. R. C. Correia, and C. Xenakis, "P2ise: Preserving project integrity in ci/cd based on secure elements," *Information*, vol. 12, no. 9, p. 357, 2021.
50. SELFKEY, "The self-sovereign digital identity wallet." `https://bit.ly/3yD8qEr`. Online; Last Accessed: 07/2023.
51. ENISA, "Cyber insurance: Recent advances, good practices and challenges."
52. D. Woods and A. Simpson, "Policy measures and cyber insurance: a framework," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 209–226, 2017.
53. P. Bountakas, K. Koutroumpouchos, and C. Xenakis, "A comparison of natural language processing and machine learning methods for phishing email detection," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pp. 1–12, 2021.
54. W. Baer, "Rewarding it security in the marketplace," *Contemporary security policy*, vol. 24, no. 1, pp. 190–208, 2003.
55. ADVISEN Transforming Insurance, "Cyber liability insurance market trends: Survey."
56. L. Joshila Grace, S. Vigneshwari, R. Sathya Bama Krishna, B. Ankayarkanni, and A. Mary Posonia, "A joint optimization approach for security and insurance management on the cloud," in *Advances in Intelligent Computing and Communication: Proceedings of ICAC 2021*, pp. 405–413, Springer, 2022.
57. M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: The role of pre-screening and security interdependence," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2226–2239, 2018.
58. J. R. Nurse, L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, "The data that drives cyber insurance: A study into the underwriting and claims processes," in *2020 International conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pp. 1–8, IEEE, 2020.
59. Z. Amin, "A practical road map for assessing cyber risk," *Journal of Risk Research*, vol. 22, no. 1, pp. 32–43, 2019.
60. S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the swedish financial sector," *Computers & security*, vol. 105, p. 102239, 2021.
61. S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity*, vol. 8, no. 1, p. tyac006, 2022.
62. U. Franke, "The cyber insurance market in sweden," *Computers & Security*, vol. 68, pp. 130–144, 2017.
63. I. goverernance, "Iso 27000 series of standards." `https://bit.ly/2zyd9eR`. Online; Last Accessed: 07/2023.
64. M. Karatisoglou, A. Farao, V. Bolgouras, and C. Xenakis, "Bridge: Bridging the gap between cti production and consumption," in *2022 14th International Conference on Communications (COMM)*, pp. 1–6, IEEE, 2022.
65. K. Kirkpatrick, "Cyber policies on the rise," *Communications of the ACM*, vol. 58, no. 10, pp. 21–23, 2015.
66. S. Mansfield-Devine, "Security guarantees: building credibility for security vendors," *Network Security*, vol. 2016, no. 2, pp. 14–18, 2016.
67. R. Anderson, R. Böhme, R. Clayton, and T. Moore, "Security economics and the internal market," *Study commissioned by ENISA*, 2008.
68. MARSH, "Covid-19: Implications for cyber, media, and tech e&o coverage." `https://bit.ly/404bMwl`. Online; Last Accessed: 07/2023.
69. AXIS INSURANCE COMPANY, "Claim supplemental application."
70. D. Woods, R. Bohme, J. Wolff, and D. Schwarcz, "Lessons lost: Incident response in the age of cyber insurance and breach attorneys," in *Proceedings of the 32nd USENIX Security Symposium*, 2023.
71. G. Mott, S. Turner, J. R. Nurse, J. MacColl, J. Sullivan, A. Cartwright, and E. Cartwright, "Between a rock and a hard (ening) place: Cyber insurance in the ransomware era," *Computers & Security*, 2023.
72. D. W. Woods and R. Böhme, "How cyber insurance shapes incident response: A mixed methods study," in *Workshop on the Economics of Information Security*, 2021.

73. D. W. Woods and J. Weinkle, "Insurance definitions of cyber war," *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 45, pp. 639–656, 2020.
74. Z. Lin, T. Sapp, R. Parsa, J. Rees Ulmer, and C. Cao, "Pricing cyber security insurance," *Lin, Zhaoxin, Travis Sapp, Rahul Parsa, Jackie Rees-Ulmer, and Chengxin Cao (2022)," Pricing Cybersecurity Insurance," Journal of Mathematical Finance*, vol. 12, no. 1, 2018.
75. World Wide Web Consortium (W3C), "Verifiable credentials json schema specification, draft community group report."
76. R. Mukta, J. Martens, H.-y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain-based verifiable credential sharing with selective disclosure," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 959–966, IEEE, 2020.
77. C. Dive, "Marriott is still covering — and recovering — expenses from its 2018 data breach." `https://bit.ly/3JFMOsd`. Online; Last Accessed: 07/2023.
78. H. Chu, P. Zhang, H. Dong, Y. Xiao, S. Ji, and W. Li, "A survey on smart contract vulnerabilities: Data sources, detection and repair," *Information and Software Technology*, p. 107221, 2023.
79. S. Aggarwal and N. Kumar, "Attacks on blockchain," in *Advances in computers*, vol. 121, pp. 399–410, Elsevier, 2021.
80. B. Putz and G. Pernul, "Detecting blockchain security threats," in *2020 IEEE International Conference on Blockchain (Blockchain)*, pp. 313–320, IEEE, 2020.
81. Ethereum Organization, "Token standards of ethereum." `https://ethereum.org/en/developers/docs/standards/tokens/`. Online; Last Accessed: 07/2023.
82. Hyperledger Foundation, "Hyperledger ursa." `https://bit.ly/3OgMYOb`. Online; Last Accessed: 07/2023.
83. Protocol Labs, "Ipfs powers the distributed web." `https://bit.ly/3ZPEtgg`. Online; Last Accessed: 07/2023.
84. Hyperledger Foundation, "Hyperledger aries." `https://bit.ly/42pFM7o`. Online; Last Accessed: 07/2023.