Crowdfunding the Insurance of a Cyber-Product Using Blockchain

Iman Vakilinia*, Shahriar Badsha[†], Shamik Sengupta[‡]
Department of Computer Science and Engineering, University of Nevada, Reno
Reno, NV, USA
Email: *ivakilinia@unr.edu, [†]sbadsha@unr.edu, [‡]ssengupta@unr.edu

***Abstract*—Organizations are interested in transferring their cyber-risks to insurers aiming to mitigate the cost of cyber-threats. However, cyber-insurance has not been widely accepted due to several obstacles. First, the lack of reliable data to measure the cyber-risks makes it hard to calculate the insurance premium. Second, there are legal and procedural hurdles for assessing the organizations security posture deterring insurer for auditing. On the other hand, the blockchain technology has been extensively popularized due to its ability to provide transparency and security. Blockchain applies the distributed ledger to store transaction histories, and the information is stored across a network of computers instead of on a single server.**

In order to improve the application of the cyber-insurance, in this research, we propose a new framework to insure a cyber-product using the blockchain technology. First, a vendor initiates a request for insuring a cyber-product, then the interested insurers participate in a sealed-bid auction by bidding their preferred premium for the insurance service. The auction winners will be selected as the insurers, and they receive tokens in return of their obligations. In the case of an indemnity request, the auditor checks the validity of a request, then calls the claim function to retrieve the corresponding amount from the funds collected from the insurers. Furthermore, we propose a new method to implement a sealed-bid auction for the insurance crowdfunding in smart contract.

***Index Terms*—Cyber-insurance, Blockchain, Crowdfunding, Sealed-bid auction**

I. Introduction

In recent years, the cyber-risks have been considered one of the most challenging issues in Information Technology (IT) sectors which could potentially lead to serious threat to individuals, businesses and organizations. With the emergence of IoT devices, networks, wireless technologies and the information technology in our daily life, IT systems and any important information related to these systems became highly vulnerable. Although the techniques that can assist organizations to identify the potential cyber vulnerabilities and improve their cybersecurity have been useful, the organizations can get more benefits by transferring the risk to other parties [1]–[4]. More specifically, a Cyber-insurance is the transfer of financial risk associated with network and computer incidents to a third party service provider known as the insurer.

On the other hand, blockchains, and their ability to represent value in the form of tokenized assets are ideal platforms for fund-raising activities. Investors can easily back innovative products, in an efficient and secure way. Crowdfunding on the blockchain can be used to speed up the investment process, reducing the time to market. Furthermore, the process is opened up to different types of investors, democratizing the fund-raising process. For these reasons, blockchain-based crowdfunding can be used to underwrite insurance policies effectively.

Another advantage of using blockchain technology is transparency. The cyber-insurance policyholders (and other stakeholders) can have unprecedented access to immutably stored data, such as information on premiums, claims or profits. Transparency provides fairness and trust, which will also help the public's perception of the cyber-insurance industry, which is often portrayed as untrustworthy.

A number of global insurers are developing alliances [5] and exploring new payment business models to achieve capital efficiencies through single global ledgers. Increased automation to capture risk data in contracts also offers new opportunities to build market knowledge, streamline payments and attract financing risk. At minimum, global insurers can use blockchain to cut asset management costs by reducing the hedging fees they pay to protect themselves from currency fluctuations in international transactions. Insurers developing these offerings typically restrict consumers options and limit the data that can be included. With the blockchain, wallets can achieve customer engagement on a much greater scale, with tailored functionalities and more integrated data. Consumers could have all their identities and insurance information available instantly.

Considering the cyber-insurance demand, and the capabilities of the blockchain technology, in this research, we propose a new framework to insure a cyber-product using the blockchain. Currently, cyber-insurance models are mainly concerned with the businesses' liability for digital assets, data breach, and business interruption [6]. However, the diversity and the extent of the IT services, makes it difficult to measure the insured's cyber-risks. In contrast, in our model the insurer insures a cyber-product. This facilitates the insured's risk estimation as the threat scopes are limited to the cyber-product. In our proposed framework, a vendor initiates a request for insuring a cyber-product, then the interested insurers participate in a sealed-bid auction by bidding their preferred premium for the insurance service. The auction winners will be selected as the insurers, and they receive tokens in return for their obligations. In the case of an indemnity request, the auditor checks the validity of a request, then calls the claim function to retrieve the corresponding amount from the funds collected from the insurers. By recording the information in the blockchain, the framework protects the integrity of the data so that malicious entities can not misuse the system.

The main contributions of this paper are the two parts, as described below:
1- We present a crowdfunding cyber-product insurance framework using blockchain technology.
2- We propose a new method to implement a sealed-bid auction for the insurance crowdfunding in the smart contract of the blockchain.

The rest of the paper is organized as follows. In the next section, we discuss the blockchain and smart contract technologies. Section III reviews major related works in the cyber-insurance and blockchain technology. The system model is presented in section IV. We introduce our proposed framework in section V. In section VI, we analyze the underlying auction mechanism for the framework. The implementation of the framework using smart contract is discussed in section VII. Finally, we conclude the paper in section VIII.

II. Blockchain and Smart Contract

The blockchain technology has been extensively popularized due to its ability to provide transparency and security. Blockchain applies the distributed ledger to store transaction histories. In this case, all network participants share the same documentation instead of individual copies, and updating records are done by consensus, which requires every nodes' agreement. Moreover, blockchain provides more security as the information is stored across a network of computers instead of on a single server. Thanks to its ability to provide a public ledger across multiple untrusted parties, blockchain has the potential to eliminate errors and detect fraudulent activity. A decentralized digital repository can independently verify the authenticity of customers, policies, and transactions (such as claims) by providing a complete historical record. As such, insurers would be able to identify duplicate transactions or those involving suspicious parties. First-moving insurers are already exploring the use of blockchain to reduce fraud and risks associated with payments across borders and transactions involving multiple currencies. In specialty insurance and reinsurance markets, where insurers are often removed from the end clients, blockchain may be used to address the considerable inefficiencies, gaps, and errors caused by poor data quality in both front and back offices.

The Ethereum blockchain [7] currently provides the highest support for smart contracts creation. Smart contracts are executed by a simple stack-based Turing complete 256-bit virtual machine known as the Ethereum Virtual Machine (EVM). Solidity is the common scripting language for writing smart contracts with a growing community. Ether represents the unit of currency in Ethereum and there are two types of accounts: externally owned accounts and contract accounts. An externally owned account is typically associated with a user, it consists of a unique public-private key pair. On the other hand, a contract account is controlled by the contract instead of a single private key. Transactions are created and signed by externally owned accounts. The receiver of the transaction can be an externally owned account or a contract account. In the former case, the transactions purpose is to transfer ethers between users. Whereas in the latter case, the transaction triggers the execution of a function on the smart contract. Transactions also include a gas limit and a gas price; the amount of gas consumed to execute the transaction is converted into ethers using the gas price. These ethers are charged to the senders account as transaction fees.

The smart contract in blockchain makes it possible to specify business logic for transactions, ranging from recording who owns which asset to executing self-enforcing and complex functions (smart contracts). The automatic transferring of assets and automatic claim processing are some of the examples of how smart contracts and blockchain can bring the advantages.

As an example of “improved asset transfer”, let's consider an example of buying a house. While buying, a mortgage lender needs to verify that the owner of a property for sale has the right to sell it and that the buyer has the right to purchase it. Currently, this process can take weeks for a title that has had prior liens on it. With the blockchain technology, this process can be done in a few seconds and save considerable cost because all of the property data can be stored in a blockchain. The data stored in a blockchain can readily identify whether the seller still owns the property and has not already sold it, and it can identify any liens on the property. The blockchain technology does the work of the middlemen in the transactions.

For another instance of “automatic claim processing” consider a smart insurance contract for trip insurance. After the airline posts a cancellation of a covered flight, it can automatically trigger a payment to those who have purchased insurance without the need to use a claims department to verify the loss. This has the potential to save the insured the hassle of filing a claim and waiting through the claims process for payment. It saves the insurer the hassle of verifying the claim.

In the case of cyber-insurance, the insurance policies are different conditions which are defined not in a trivial way and as insurers goal is usually to pay policyholders as less as possible, which dissatisfies the customers having not enough knowledge or experience about the insurance. On the other hand, customers may perform fake claims, lie and cheat to get the payout. Using the help of smart contract, if the policies are written as codes and executed without human interventions as well as decentralized way, the challenges of fake claims by the policyholders and making fewer payments by the insurers can be avoided easily.

III. Related Work

Cyber-insurance domain currently is mainly limited to the business' liability for digital assets, data breach, and business interruption [1], [6]. In contrast, in this paper, we propose a new model of the cyber-insurance to transfer the risk of a new security vulnerability exploitation of a cyber-product. We discuss the benefits of this model in section V. To achieve this goal, we apply the crowdfunding auction. The crowdfunding can be seen as an open call to provide financial resources [8].

On the other hand, recently, plenty of research studies have been done to discuss the benefits of the blockchain [9]. The

[10] proposed an architecture of blockchain platforms for insurance-related products. Specifically, it covers the market perspective of a platform as well as outlines the agreement on core platform and its API governance concepts. The smart contracts have been used to provide consensus management to manage risk pools, underwriting and claims processing. The [11] showed how the peer-to-peer nature of blockchain can benefit the insurance and why we should use them. For instance, it can help manage the crowdfunded insurance model.

The [12] presented a blockchain based cyber-insurance for continuous monitoring and processing the insurance system. Their system leverages the automated nature of smart contracts on the insurer side, decoupled from the payment aspect of the blockchain between customers and insurers. They also proposed to achieve confidentiality of the information stored in the system in different ways such as private channels within the permissioned blockchain network. In contrast, we propose a crowdfunding insurance framework to insure a cyber-product in a public blockchain. As far as the authors' knowledge, our work is the first to propose a blockchain-based crowdfunding framework for a cyber-product insurance.

Although there are not many research studies exist on blockchain based cyber insurance, there are plenty of white papers which suggested to use blockchain in the insurance for automation of payment [13], improved assets transfers [14], automatic claim processing [15], limiting fraud [16], enabling a shared view of policy information [17] and reducing administrative costs [18].

On the other hand, despite the advantages of the blockchain and smart contracts, currently, they do not sufficiently protect the transactional privacy. Hence, recently several works have been done to improve the blockchain transactional privacy. Zcash [1] and Monero [2] are privacy-preserving cryptocurrencies. However, they do not support programmability. Kosba et al. [19] have presented Hawk a decentralized smart contract system to protect the transactional privacy. However, Hawk needs a trusted setup and it is not applicable to the current smart contract model. Galal et al. [20] have presented a partially privacy-preserving verifiable sealed-bid auction smart contract on the Ethereum blockchain to protect the bids of the losers. The proposed scheme requires the bidders to initially deposit a constant value which limits the crowdfunding process as we discuss in section VII. In contrast to previous works, we present a new method for implementing the insurance crowdfunding sealed-bid auction which we discuss with more details in section VII.

IV. System Model

In this section, we describe the system model in our proposed cyber-insurance framework. In this model, the insured is a cyber-product. Such cyber-products can be a software, hardware, network, application, or even a service. In the rest of the paper, we refer to an insured as a cyber-product. There are four entities participating in this model which are *Vendor*, *Customer*, *Auditor*, and *Insurer*. These entities are described as follows:

Vendor- A vendor is the requester of the insurance service for its cyber-product to transfer the risk of the exploitation of a new vulnerability to another party namely the insurer. The vendor can be a software/hardware producer, application developer, IT service provider, and etc. The vendor's goal is to acquire a larger share of the market by providing the insurance service to the customers. The framework should ensure that the vendor does not decrease its security investment for the detection of the new vulnerabilities.

Customer- A customer is the end-user of the cyber-product. The customer buys the product from the vendor while expecting a desired security level for the cyber-product to be safe from cyber-attacks. Customers prefer cyber-insurance for the cyber-product to receive reimbursement in the case that the attackers exploit a new vulnerability.

Auditor- An auditor is responsible for assessing the security of the cyber-product. Furthermore, the auditors are responsible for checking the validity of the customers' indemnity requests. The system should be designed in a way to prevent the collusion between the auditors, customers, and vendors.

Insurer- An insurer is an entity accepting the risk of the cyber-product's security against the new vulnerabilities in return for a premium. Insurers are risk seekers agents considering the cyber-product's security level to participate in the insurance process.

A. Design Objectives

The motivation for the design of a cyber-product insurance are as follows:

- *Cyber-product Insurance:* Having the cyber-product insurance, makes the customers more confident about the cyber-product's security and compensates the cost of cyber-attacks. This increases the market share for the vendor.
- *Risk Sharing:* As it is hard to calculate the probability of the exploitation of a product's new vulnerability, the insurers might not be interested in accepting the whole risk and thus investing on such market. However, by designing a crowdfunded insurance platform, and risk pooling, the low-risk tolerance insurers are motivated to invest in such a process as well.
- *Improve Security:* The mechanism should entail the improvement of the cyber-product's security.
- *Transparency:* The framework should transparently demonstrate the product's security status, the vendor's effort toward security, and the auditor's efficiency in evaluating the cyber-product's security.

B. Challenges

As the agents are strategic, they tend to maximize their utilities which causes the deviation from the social welfare point. The system design should consider the following challenges:

- *Collusion Resistant:* The system should prevent the malicious entities to collude with each other. For example, an auditor might collude with a vendor to evaluate a product

[1] https://z.cash/

[2] https://monero.org/

as secure with the goal of decreasing the insurance premium.

- *Moral Hazard and Adverse Selection:* Moral hazard refers to the case where a vendor decreases its security investment after getting the insurance. On the other hand, adverse selection is caused by the information asymmetry between the insurers and vendors causing the insurer to improperly evaluate the probability of the product exploitation [1], [6].

V. Crowdfunding Cyber-Insurance Framework

In this section, we elaborate our proposed framework for the crowdfunding cyber-product's insurance using the smart contract on the blockchain. The proposed framework is consisted of three components, namely *Registration*, *Crowdfunding*, and *Indemnity* which we explain them in the following.

Registration- First, the vendor provides the necessary information about the cyber-product's security. This requires a vendor to publish the necessary documents to the auditors and insurers. This information includes the security certificates such as Common Criteria, FIPS-140, PCI-DSS, and ISO 27000 series. For instance, consider Common Criteria which is an international standard (ISO/IEC 15408) for computer security certification. Although it does not guarantee security, it can ensure that claims about the security attributes of the evaluated product were independently verified. In other words, products evaluated against a Common Criteria standard exhibit a clear chain of evidence that the process of specification, implementation, and evaluation has been conducted in a rigorous and standard manner. Common Criteria has different Evaluation Assurance Levels (EALs) where the higher EAL demonstrates a more secure product [21]. Furthermore, the vendor can request auditors for more detailed auditing of the product. The auditors evaluate the security level of the product by investigating the documents, specifications, and the implementations. More detailed security investigation brings more certainty about the product's security level. Besides that, a vendor can request several auditors to increase the certainty. Afterward, the auditors register the product's security information in the blockchain which is accessible by the public. Auditors use their private-keys to sign such information.

Crowdfunding- Once, the security information has been published in the blockchain, the vendor starts the auction process. Our framework applies the sealed-bid auction for this purpose. This is due to the fact that in the sealed-bid auction the insurers bid based on their true valuations instead of bidding according to the current auction status. As the auction process is a smart contract over the blockchain, the users are ensured that the vendor is not cheating in the auction process.

Insurers participating in the sealed-bid auction by representing the value they would obligate for the insurance, and the corresponding requested premium for their obligation. Once the auction is over, the winners will be selected based on the total demanded indemnity for the insurance. Then, the smart contract supplies the winners the tokens in return for their obligations. The insurers will be reimbursed their obligations by returning these tokens at the end of the insurance contract. Moreover, the insurers can sell their tokens during an insurance policy. This brings more liquidity for the insurance system attracting more insurers to the system.

Indemnity- If no vulnerability exploited during the time of the insurance policy, the insurers return their tokens and will be reimbursed their obligated values. In the case of the exploitation of a new vulnerability, the customers first report it to the vendor and the auditor. Then, they register this information into the blockchain, after validation of the information, the auditor calls the reimbursement function to extract indemnity from the crowdfunding phase. The indemnity cost will be fairly divided between insurers.

The claiming process is recorded on the blockchain and has negative effects on the vendor's credit causing less trust to the vendor's security. This increases the insurance premium and makes fewer insurers willing to participate in the product's insurance.

Figure 1 depicts the entities and their interaction with the blockchain.

Advantages of Proposed Framework

In the following, we discuss the advantages of the proposed framework, and how it alleviates the challenges mentioned in section IV-B.

- As it is hard to calculate the risk encountering the cyber-product, the insurers might not accept a large indemnity request. However, by applying an insurance crowdfunding, the insurers diffuse the impact of loss by risk pooling. This motivates the insurers with different risk tendency to select their desired risk level.
- Blockchain transparently records the claims and indemnities allowing the insurers to monitor the insureds' performance. Although measuring the risk of exploitation of a new vulnerability is hard for the insurers, the vendor's efficiency for handling security issues over time helps insurers to make a better decision for their investment, and such design leverages the provision of entities' reputation. This alleviates the moral hazard and adverse selection since a vulnerability exploitation is recorded in the blockchain causing credit loss for a vendor and the corresponding auditors. Moreover, the transparency and the integrity of the blockchain alleviates the entities collusion with the same reason.
- In the traditional insurance models, it is hard or even impossible for the insurers to transfer the risk of the insurance service to another party. However, applying the smart contract, insurers receive tokens (i.e. ERC20 tokens for the Etherium) for their obligations. In this case, the insurers can sell their tokens to other insurers. The insurers will be reimbursed their obligations once the contract is over.
- The entities are confident about the correct execution of the smart contract, as it executes in the public blockchain backed by a consensus mechanism. The blockchain design also eliminates the role of brokers. This increase the entities' utilities.

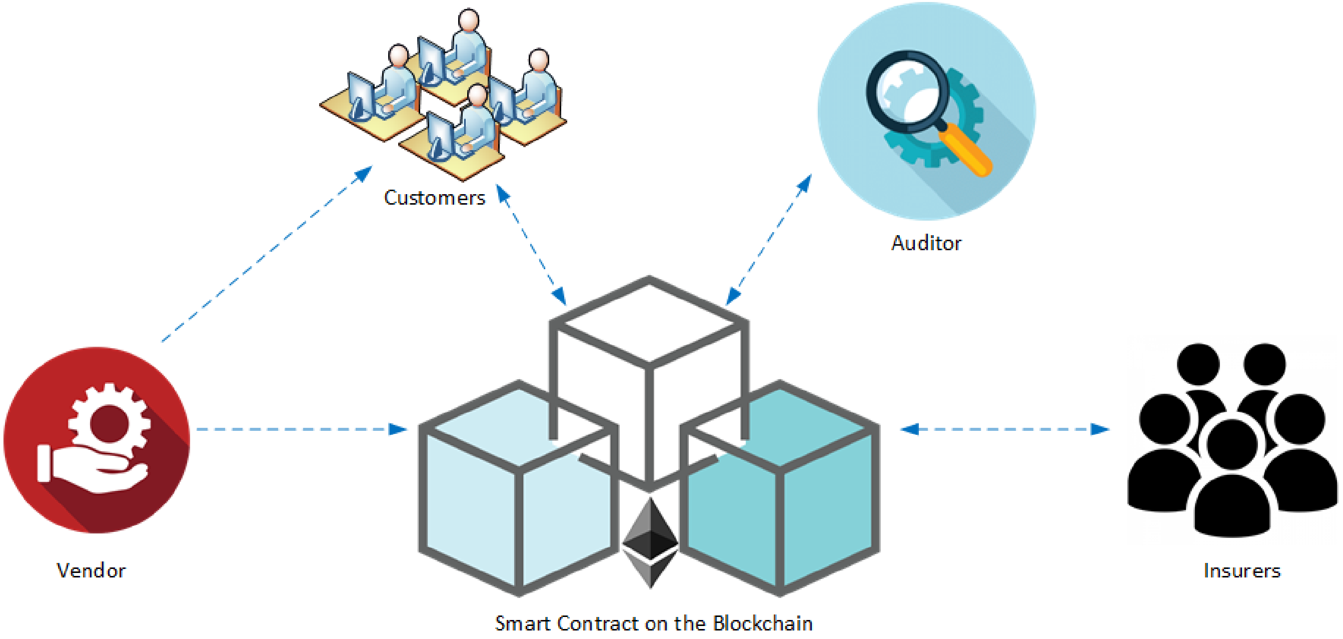

Fig. 1: Crowdfunding the insurance of a cyber-product

VI. Insurance Crowdfunding Auction

In this section, we analyze the insurers' bidding strategy in the crowdfunding process.

Let π represent the premium a vendor needs to pay for the insurance service to an insurer. The insurance is *actuarially fair* if $\pi = p \times l$, where p denotes the probability of a new vulnerability exploits by an attacker and l represents the indemnity value that an insurer is obligated to pay [1]. Note that the measuring of p is challenging and it depends on many variables such as the attack vectors and threat models, the customers' business, the sensitivity of the underlying data that the cyber-product interact with it, and the scope and the number of the customers. For example, a banking application is a good target for the attackers while attackers might not be interested in to invest in finding a new vulnerability for a video game. In the full coverage setting, the insurer should pay the whole cost of damage. However, in our design, the vendor usually applies for the partial coverage mainly because it is hard to calculate the cost of exploitation for the customers. The vendor guarantees a threshold value as the indemnity if a new vulnerability exploited.

For simplicity and without loss of generality, consider that there is one coin for the obligation which is going to be sold in the crowdfunding insurance framework. Let R denote the maximum premium the vendor would pay to the insurer. In other terms, the premium higher than R is not profitable for the vendor. Let L represent the least premium value which is profitable for an insurer. Thus, we can represent $X \in (L, R)$ as a set of the possible values for a premium which results in the positive utility for an insurer $u(x \in X) \rightarrow \mathbb{Z}^{+}$. Assume N represents the total number of auction participants (insurers), and let Y represent the number of auction winners ($Y < N$). Having the same profit for the insurers, then we have the following proposition.

Proposition 1. Assuming the insurers bid b uniformly random from X, formally $\forall x_1, x_2 \in X, x_1 \neq x_2, Pr(b = x_1) = Pr(b = x_2)$, then an insurer's expected utility is

$$E[u] = b.(\frac{R-b}{R})^{(N-Y)} \tag{1}$$

Proof. A bidder's expected utility is the amount of its requested premium multiplied by the probability of the winning the auction. As the bidders bid uniformly random in the range of (L, R), the probability of the winning is $(\frac{R-b}{R})^{(N-Y)}$ □

Proposition 2. Following the proposition 1, the insurer's best response strategy is to bid

$$b^{*} = (\frac{R}{N-Y+1}) \tag{2}$$

Proof. As the second derivative of the equation 1 is negative, we calculate the first order condition of the equation 1 to find the b^{*} which maximizes the $E[u]$.

$$\frac{\partial(b.(\frac{R-b}{R})^{(N-Y)})}{\partial b} = 0$$

$$(\frac{R-b^{*}}{R})^{(N-Y)} + (N-Y)(\frac{R-b^{*}}{R})^{(N-Y-1)}(\frac{-b^{*}}{R}) = 0$$

$$(\frac{R-b^{*}}{R})^{(N-Y-1)}(\frac{R-b^{*}}{R} + (N-Y)(\frac{-b^{*}}{R})) = 0$$

$$(\frac{R-b^{*}-Nb^{*}+b^{*}Y}{R}) = 0$$

$$b^{*} = (\frac{R}{N-Y+1})$$

□

As it can be seen from the proposition 2, with the increase of maximum premium value R, and the number of auction winners Y, an insurer's bid increases as well, however with the increase of the total number of bidders N, the insurers decrease their bid to increase the chance of winning.

VII. Implementation of the Crowdfunding Auction using Smart Contract

As the transactions are transparent in the blockchain, the implementation of the sealed-bid auction for crowdfunding is challenging. To assure the payment from the auction winners, the bidders should transfer their bid values to the smart contract in the bidding phase. However, this is challenging mainly because storing bids in the blockchain can be read by the public. This causes bidders to change their bids accordingly, and not bid truthfully causing the profit loss for the vendor. For example, assume for an insurer a true valuation of an insurance service is \$1 premium, once the insurer notifies the lowest requested premium is \$2, then the insurer decreases the bid to \$1.99 to win the auction.

To overcome this problem, we implement the auction process in two separate phases as `bidding` and `revealing`. We apply the commitment scheme to protect the bid values. A commitment scheme has hiding and binding properties. Hiding requires that a commitment does not reveal any information about the committed value, and binding property guarantees that a commitment cannot be opened to another value. For our implementation, we have used Ethereum-SHA3 hash function (Keccak256) as the commitment scheme.

A naive method to protect the transaction privacy in the sealed-bid auction is to enforce bidders to transfer a constant amount higher than all of the possible bids [20], then the smart contract reimburses participants once the auction is over. However, this solution is not applicable to our problem for one main reason. The constant value might be so large restraining many bidders to participate in the crowdfunding process. For example, consider that the crowdfunding needs $\$1,000,000$, thus using the naive model, the auctioneer sets the constant value to $\$1,000,000$. In this case, the small retailers which cannot afford the initial payment of $\$1,000,000$, are eliminated from the auction. To overcome this problem, in our proposed model, we do not require the transferring of a constant value for the auction entrance. In our proposed model, each bidder transfers an amount which is the combination of its demanded obligation of the insurance and the corresponding premium. This allows every insurer with different investment tendency to participate in the auction process.

Let K represents the coverage that a bidder would obligate for the insurance, and x is its demanded premium. Note that in the auction of the insurance framework explained in the previous section, insurers need to provide the amount of their coverage and also their proposed interest rate. Thus, the bidders need to transfer their proposed coverage. However, in order to protect their premium value, we require the bidders to transfer $T = K - x$ to the smart contract. This indicates that the bidder is deducting its asked premium from the transaction. In this case, although the transaction value T is readable by the public, it is not possible to infer K and x values, whereas the latter value is the sensitive parameter of the auction. On the other hand, bidders should prove that they will not change their proposed x value after the bidding process. Thus, bidders should submit a commitment of their bid values in the bidding phase as well. To this end, each bidder selects a random secret nonce value s, and computes $C = Comm(s||x)$, then submits C to the smart contract in the bidding phase.

Once the bidding time is over, the bidders call the revealing function by opening their committed values. To this end, bidders send $\{x', s', K'\}$ to the smart contract in the revealing phase. The smart contract computes $Comm(s'||x')$ and checks if it is equal to the C. Moreover, the smart contract checks if $T = K - x'$ holds. If the bidder has honestly followed the protocol, then the bid value will be registered into the blockchain. Note that as in the bidding phase, the bid's commitment has been registered in the blockchain, it is not possible to change these values afterward. Then the vendor selects the winners and sends them tokens in return of their obligations, and the losers will be reimbursed their committed bids. We apply ERC20 token which is a standard for smart contracts on the Ethereum blockchain for implementing tokens. Since the on-chain calculation of the winners is costly mainly because of sorting, it is better to offload this operation off-chain. Since the revealing transactions are recorded in the blockchain, the vendor can not cheat in the selection of auction winners, and such computation can be verified publicly.

In the following, we explain the algorithms for the proposed framework.

`setup`: The vendor initializes the crowdfunding smart contract settings by deploying this function. This constructs the contract by receiving the following parameters: T_1 (Bidding time interval), T_2 (Revealing time interval), $token$ (The number of ERC20 tokens which will be given to the auction winners in return of their obligations, these tokens will be reimbursed at the end of the insurance contract, moreover these tokens can be sold to other entities), $maxPremium$ (The maximum acceptable premium rate)

`bidding`: Insurers call this function to bid in T_1. Bidders first calculate their T and C as described, and then transfer and submit T, and C (the bidder commitment) to the bidding function. Once the T_1 is over, all of the bids have been registered in the blockchain ledger.

`revealing`: Insurers reveal their bid values and winners will be selected. For this purpose, the bidder submit $\{x', s', K'\}$ as explained, and the contract computes and checks the validity of C, and T.

`wrapping`: Auction winners receive tokens and losers will be reimbursed by their transacted values. Note that, as the on-chain computation is costly, this part can be done off-chain to reduce the gas cost. As in the revealing phase, the bid values are registered in the blockchain ledger, the winners selection can be verified by the public disallowing the auctioneer to collude with bidders. Once the winners have been selected, they receive corresponding tokens and losers reimburse their initial transactions T.

`indemnity`: Customers request indemnity by calling this function. In this case, the customers submit their evidence of exploitation into the blockchain. Once the information has been uploaded, the vendor and the auditor verifies the information, and the auditor reimburses the customers from the fund obtained in the crowdfunding phase.

TABLE I: Gas cost for the auction function

Function	Gas units	Gas cost (USD)
codeDepositCost	185200	0.1355
executionCost	100960	0.0738
maxPremium	406	0.0002
T1	494	0.0003
T2	450	0.0003
C	462	0.0003
x’	616	0.0004
token	575	0.0004
bidding	40567	0.0296
transaction	506	0.0003

We have uploaded the solidity code of the smart contract for the sealed-bid crowdfunding auction at `https://github.com/imanvk/crowdfundingInsuranceAuction`. We have used the *remix* for the compiling of the contract code. Table I demonstrates the gas cost for our auction implementation. The ether price in $09/02/2018$ is $\$292.71$, and the gas cost is 2.5 Gwei where 1 ether = 10^9 Gwei. As it can be seen, from table I, the implementation of our proposed model is practical.

VIII. Conclusion

In this paper, we have proposed a new framework for insuring a cyber-product using the blockchain technology. To share the risk of insurance, we have applied a crowdfunding through a sealed-bid auction process. We have discussed the advantages of our proposed framework, and analyze the bidding strategy of the insurers. Finally, we have studied the implementation of a sealed-bid auction on the blockchain, and we proposed a method to preserve the bid values during the bidding process.

References

[1] L. A. Gordon, M. P. Loeb, and T. Sohail, “A framework for using insurance for cyber-risk management,” *Communications of the ACM*, vol. 46, no. 3, pp. 81–85, 2003.

[2] T. Moore, “The economics of cybersecurity: Principles and policy options,” *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 103–117, 2010.

[3] D. K. Tosh, I. Vakilinia, S. Shetty, S. Sengupta, C. A. Kamhoua, L. Njilla, and K. Kwiat, “Three layer game theoretic decision framework for cyber-investment and cyber-insurance,” in *International Conference on Decision and Game Theory for Security*. Springer, 2017, pp. 519–532.

[4] D. Geer, “Risk management is still where the money is,” *Computer*, no. 12, pp. 129–131, 2003.

[5] M. Swan, *Blockchain: Blueprint for a new economy.* ” O’Reilly Media, Inc.”, 2015.

[6] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, “Cyber-insurance survey,” *Computer Science Review*, vol. 24, pp. 35–61, 2017.

[7] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[8] P. Belleflamme, N. Omrani, and M. Peitz, “The economics of crowdfunding platforms,” *Information Economics and Policy*, vol. 33, pp. 11–28, 2015.

[9] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, “Consensus protocols for blockchain-based data provenance: Challenges and opportunities,” in *Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017 IEEE 8th Annual*. IEEE, 2017, pp. 469–474.

[10] S. Chekriy and Y. Mukhin, “i-chain.net.wpaper_rev_005,” https://i-chain.net/i-chain.net.wpaper_rev_005.pdf, May 2018, (Accessed on 09/03/2018).

[11] O. Rikken, “Why blockchain could enable a true p2p insurance model - coindesk,” https://www.coindesk.com/blockchain-p2p-insurance-models/, April 23 2016, (Accessed on 09/03/2018).

[12] T. Lepoint, G. Ciocarlie, and K. Eldefrawy, “Blockcisa blockchain-based cyber insurance system,” in *Cloud Engineering (IC2E), 2018 IEEE International Conference on*. IEEE, 2018, pp. 378–384.

[13] K. Wang and A. Safavi, “Blockchain is empowering the future of insurance,” Oct 2016. [Online]. Available: https://techcrunch.com/2016/10/29/blockchain-is-empowering-the-future-of-insurance/

[14] “Blockchain: An insurance focus - milliman insight,” http://www.milliman.com/insight/2016/Blockchain-An-insurance-focus/, (Accessed on 09/03/2018).

[15] R. Huckstep, “What does the future hold for blockchain and insurance?” Jan 2016. [Online]. Available: https://dailyfintech.com/2016/01/14/what-does-the-future-hold-for-blockchain-and-insurance/

[16] T. S. U. A. News, “Bitcoin flaws beckon hackers,” Apr 2015. [Online]. Available: https://www.infosecurity-magazine.com/news/bitcoin-flaws-beckon-hackers/

[17] “Insurance industry making the leap to blockchain — business insurance,” https://www.businessinsurance.com/article/20170620/NEWS06/912314004/Blockchain-AIG-IBM-Standard-bank-broking-Bitfury-insurers-brokers-, (Accessed on 09/03/2018).

[18] “Blockchain in insurance–opportunity or threat? — mckinsey,” https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat, (Accessed on 09/03/2018).

[19] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[20] H. S. Galal and A. M. Youssef, “Verifiable sealed-bid auction on the ethereum blockchain.”

[21] “Common criteria,” https://en.wikipedia.org/wiki/Common_Criteria.