# Dynamic Value Asymmetry in Ransomware Models: Resolving Limitations in Vakilinia et al.

Akintoye Oyedola
*School of Computing*
*University of North Florida*
Jacksonville, Florida, USA

***Abstract*—Ransomware remains a critical cybersecurity threat, imposing severe operational and economic losses on organizations. This paper revisits the 2021 mechanism design framework of Vakilinia et al. for smart contract-based ransomware negotiation and demonstrates that key modeling assumptions limit its practical applicability, particularly in real-world bargaining environments with shifting and asymmetric valuations. Specifically, the analysis formalizes two research gaps: the neglect of scenarios in which the attacker's minimum acceptable payoff exceeds half of the victim's true valuation, and the treatment of the victim's valuation of encrypted data as a static quantity despite time-dependent business interruption costs. To address these gaps, the paper introduces a dynamically parameterized mechanism that embeds temporal depreciation of the victim's valuation and explicit value asymmetry into the game-theoretic structure, while preserving incentive compatibility for both parties. The resulting framework yields more realistic equilibrium outcomes, improves the stability and fairness of ransomware negotiations, and strengthens the viability of smart contract-based approaches in the absence of a trusted third party.**

***Index Terms*—ransomware, negotiation, smart contract**

## I. Introduction

Due to technological advancements, ransomware is one of the most disruptive problems organizations face today. Ransomware attacks cause technical damage and chaos when operations come to a sudden stop. This results in business interruption costs due to lack of access to encrypted data and loss of stakeholders' trust. Even when companies have decent backups, they often find it difficult to negotiate directly with the attacker to regain access to encrypted data. Furthermore, ransomware negotiation is a lengthy process due to the limited communication channels between attackers and victims. Differences in valuation also prolong negotiation efforts, increasing business downtime. In addition, attackers and victims need a mediator to oversee communication and the exchange of ransom and decryption key. However, it is illegal in all countries to collaborate with criminals. This complicates the search for a trusted third party (TTP) entity to handle the communication and exchange. Most victims end up improvising and attackers take advantage of that uncertainty. Thus, ransomware attacks remain a growing cybersecurity threat. Although there are extensive studies on ransomware prevention, it is important to provide effective frameworks for ransomware negotiation that reduce business interruption costs for the victim. Recent ransomware negotiation research focus on game-theoretic models and smart-contract concepts that attempt to shorten the negotiation process in the absence of a TTP. However, much of that work remains theoretical and has consequential research limitations. I study the **2021 Mechanism Design Approach** proposed by Vakilinia et al. [1] to identify and address research gaps that threaten the practical implementation of a smart-contract-based ransomware negotiation approach.

Vakilinia et al. designed a negotiation facilitation mechanism between ransomware attackers and victims with the explicit goal of reducing business interruption costs. First, the authors define two ransomware dilemmas and provide solutions that force both the attacker and the victim to cooperate in a timely manner. Then, they introduce a smart contract-based solution to eliminate the need for a trusted third-party to mediate ransomware negotiations.

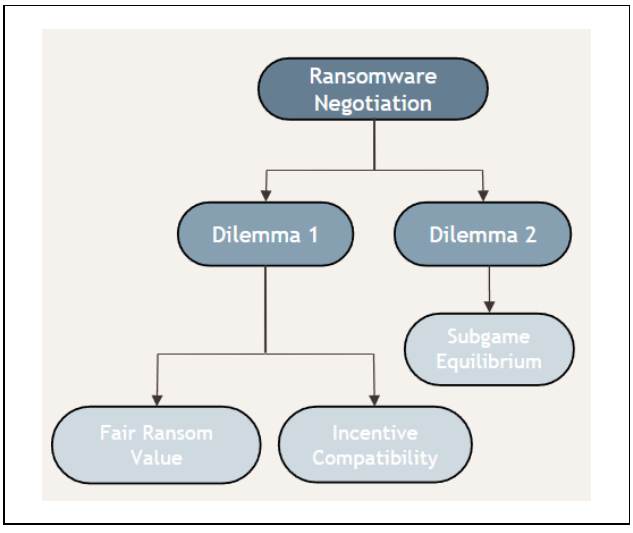


Fig. 1. Vakilinia et al.'s Mechanism Design Approach

The first dilemma is the classic "no-trust" ransomware stalemate: the victim hesitates to pay because there is no guarantee the attacker will provide the decryption key, while the attacker hesitates to reveal the decryption key before payment because the victim could then defect and not pay. Vakilinia et al. propose a mechanism design smart-contract that forces both attacker and victim to lock collateral on-chain. If either party deviates, the deviator loses their deposit,

making honest completion of the ransom exchange the rational equilibrium outcome and resolving the original trust problem.

The second dilemma is a specific scenario where the choices of the attacker or victim lead to an inefficient outcome that prolongs the negotiation process indefinitely. The proposed solution defines a game-theoretic structure that forces both parties to participate in a timely manner for joint resolution. This structure ensures that rational behavior by the parties leads to a more desirable or stable outcome that resolves the dilemma.

The core limitations of Vakilinia et al.'s approach are listed below.

1) The proposed framework does not account for a situation in which the attacker's minimum acceptable value for encrypted data exceeds half of the true victim's value. This can be visualized as a mathematical expression:
$$V_{min} > \frac{\delta}{2}$$
2) Although Vakilinia et al. focused on a smart-contract mechanism to reduce business interruption for the victim during negotiation, the proposed solution does not account for changes in the victim's original valuation of the encrypted data. Specifically, the victim incurs additional losses during downtime that reduce their original valuation of the encrypted data. Thus, the true value $\delta$ is a dynamic variable. This analytical oversight compromises the shapely value and, consequently, the fair ransom value as time passes. Similarly, the attacker lacks sufficient incentives to continue participating in the smart contract negotiation process as the victim's $\delta$ declines.

This paper closes the research gap by addressing and resolving these limitations of recent literature relevant to ransomware negotiation models. The rest of the paper is organized as follows. The next section describes the original game-theoretic dilemmas and solutions. In Sect. III, I introduce a modified mechanism that addresses each of those research gaps. I discuss limitations of the new model and outline possible extensions in Sect. IV. Finally, I conclude my paper in Sect. V.

## II. Background

The first dilemma in the Vakilinia et al.'s proposed ransomware design mechanism is to determine a fair ransom value in the absence of a TTP [1]. Since the main goal of this paper is to minimize business interruption costs during ransomware negotiation, the traditional negotiation method of sourcing and using a TTP to mediate attacker-victim interactions is too costly. Normally, an attacker does not know the true value of the victim's data. Similarly, a victim does not know the minimum value that can satisfy the attacker. Thus, negotiation between parties is time-consuming, causing additional business interruption for the victim [2]. The proposed solution involves analyzing the **Shapely Value (S.V.)** of a game model between parties to calculate a fair ransom value. S.V., a fair allocation method, divides the surplus among players in a coalition.

$$\phi_i(N) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!}(v(S \cup \{i\}) - v(S)) \tag{1}$$

Vakilinia et. al proved that the S.V. of the attacker and victim are equal, and it is half of the benefit that the victim earns after data decryption [1].

$$\phi_i(N) = \frac{\delta}{2} \tag{2}$$

Secondly, a proposed incentive-compatible mechanism should help each party get the best result for themselves. Vakilinia et al. tested a double-sided-blind auction mechanism to achieve incentive-compatibility. This means both the attacker and victim are willing to participate in the absence of a TTP. This is theoretically proven under the proposition that the S.V. $\frac{\delta}{2}$ remains the best victim response strategy in a ransomware negotiation scenario.

Thus, calculating a fair ransom value via the Shapely Value formulae and using a double-sided blind auction provides the framework for ransom value negotiation without a Trusted Third Party [3].

The second dilemma in the proposed ransomware design mechanism is to ensure that the equilibrium outcome of any ransomware negotiation is for the victim to pay a ransom and the attacker to release the decryption key for the encrypted data. Since it is not guaranteed that the attacker shares the decryption key once the victim pays the ransom, it is crucial to design a mechanism without a TTP that forces the attacker to transfer the legitimate decryption key to the victim after payment. Vakilinia et al. proved a Subgame Perfect Equilibrium of their proposed mechanism is ("Pay Ransom, Share Key, Confirm"), using a theta value ($\theta$). Theta is defined as the *earnest-money* value. This is an amount that the victim pays in addition to the ransom to convince the attacker to release a decryption key. Essentially, theta ($\theta$) encourages the victim to verify the validity of the key so the attacker can receive the ransom; then, the victim can receive their earnest-money back. The full amount paid is then represented as

$$R = r + \theta \tag{3}$$

where *R* is the full amount the victim pays, *r* is the ransom, and $\theta$ is the earnest-money value.

## III. Modified Theoretical Approach

This section presents a novel approach to resolve the research limitations outlined in the Introduction, Sect. I.

*1) Dilemma 1: Attacker's Min Value Exceeds S.V.:* The proposed frameworks in section II assume that both parties, the attacker and victim, act in good faith with mutually beneficial action plans. This negotiation logic states that $V_{min}$ is a lower value than $r$ which is a lower value than $\frac{\delta}{2}$.

$$V_{min} < r < \frac{\delta}{2}$$

where $V_{min}$ is the attacker's minimum acceptable value to release the decryption key; $\boldsymbol{r}$ is the ransom; and $\frac{\delta}{2}$ is the half of the victim's true valuation of the encrypted data.

This logic relies on the minimum acceptable value $V_{min}$ to be less than half of the true victim's valuation of the encrypted data $\frac{\delta}{2}$. However, the relevant previous literature does not account for the situation where $V_{min}$ exceeds $\frac{\delta}{2}$. This can be visualized as a mathematical expression:

$$V_{min} > \frac{\delta}{2}$$

In this scenario, the ransom $r$ will be an inadequate payment for the attacker to agree to release a decryption key. Additionally, this difference in value extends the negotiation process, further increasing the business interruption costs for the victim.

Proposed Solution:

I propose a mechanism design that creates time-based executable functions in the smart-contract to address the

$$V_{min} > \frac{\delta}{2}$$

dilemma. First, use a decentralized automation network like **Chainlink Automation** to monitor smart contract conditions and execute a function at specified intervals. Decentralized Automation Networks are a reliable and decentralized way to schedule actions since smart-contracts cannot process self-executing timer codes. Then specify the conditions for the attacker and the victim to participate and produce a position: $V_{min} < r < \frac{\delta}{2}$. The image below illustrates the source code workflow:

As illustrated in 1, the **count** variable is a global timer countdown for 48 hours. This influences both parties to participate in the negotiation process quickly, consequently minimizing business downtime and managing business interruption costs. The rest of the logic of the smart-contract function is given below.

- Within 4 hours, request a lower $V_{min}$ from the attacker. This new value is at least 10% lower than the current value.
- Within 4 hours, request a higher $\frac{\delta}{2}$ from the victim. This new value is at least 10% higher than the current value.
- Compare both values. Repeat the loop within the global **count** timer if $V_{min} > \frac{\delta}{2}$.
- Update the values of $V_{min}$ and $\frac{\delta}{2}$ by 20% if $V_{min} > \frac{\delta}{2}$ after the 48 hour period. Repeat the first 3 steps.

Specifying a minimum 10% decrease in $V_{min}$ allows the attacker to reduce their expected income while minimizing the number of reduction requests from the smart contract. This facilitates a scenario where $V_{min} < \frac{\delta}{2}$ in a timely manner.

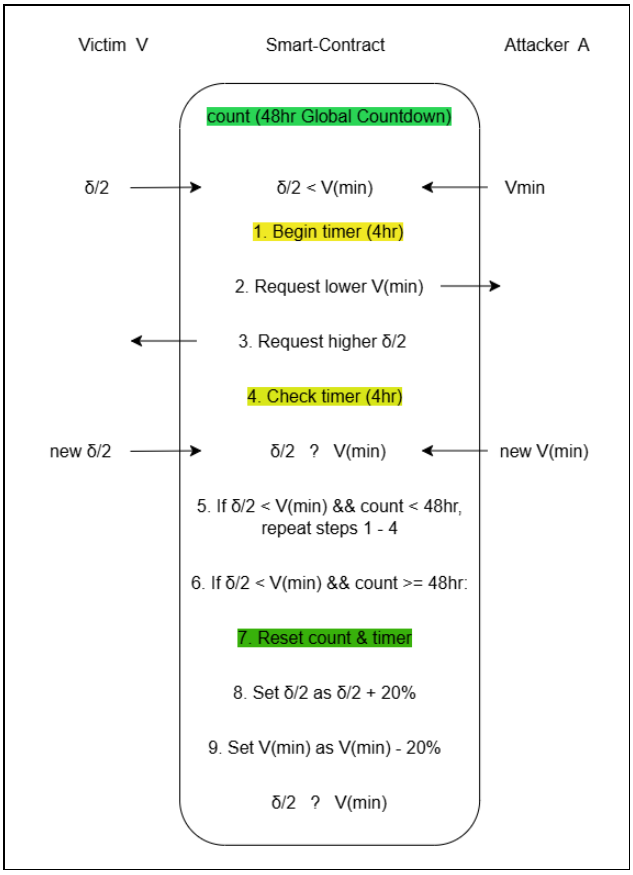


Fig. 2. Solution Workflow For Dilemma 1

Similarly, specifying a minimum 10% increase in $\frac{\delta}{2}$ prevents the victim from acting in bad faith to undermine the true value of encrypted data. This also facilitates the desired scenario in a timely manner. 10% is a proportion significant enough to alter the submitted values without fully discouraging both parties from participating in the negotiation process.

Impacting both values by 20% is a steep but necessary feature aligned with the project goal of minimizing business interruption costs for the victim via prompt resolution. This is needed before repeating the whole negotiation loop. The result is the attacker committing to a minimum acceptable payment, which accelerates the calculation of the ransom.

This solution, if included in a smart-contract for ransomware negotiation as proposed by Vakilinia et al. [1], resolves the

$$V_{min} > \frac{\delta}{2}$$

research gap which was never addressed in the original paper.

*2) Dilemma 2: Dynamic Valuation Asymmetry:* Although Vakilinia et al. focused on a smart-contract mechanism to reduce business interruption for the victim during negotiation, the proposed solution does not account for changes in the victim's original valuation of the encrypted data. Specifically, the victim incurs additional losses during downtime that reduce their original valuation of the encrypted data. Thus, the

true value $\delta$ is a dynamic variable. This analytical oversight compromises the shapely value and, consequently, the fair ransom value as time passes. Similarly, the attacker lacks sufficient incentives to continue participating in the smart contract negotiation process as the victim's $\delta$ declines.

This limitation can be addressed by treating the victim's valuation $\delta$ as a time-dependent quantity and then updating the mechanism to reflect how incentives and "fair" payments evolve over the course of the negotiation. Rather than assuming a single static value, the framework explicitly traces how $\delta$ changes as downtime losses accumulate.

*a) Modeling $\delta$ as Time-Varying:* To capture this effect, the constant valuation $\delta$ is replaced by a function $\delta(t)$ that decreases over negotiation time, reflecting the fact that prolonged downtime steadily erodes the victim's true valuation of the encrypted data. A simple linear specification such as

$$\delta(t) = \delta_0 - ct$$

can be used for illustration, although more general convex or concave decay functions may be adopted when business-interruption costs are nonlinear. Once $\delta(t)$ is introduced, the Shapley value or any other cooperative-game allocation rule is recomputed in terms of $\delta(t)$, so that the fair ransom becomes a time-indexed function $R(t)$ that automatically accounts for the shrinking surplus as negotiations drag on.

*b) Redesigning Incentives for Both Parties:* The mechanism must then be adjusted so that both players' incentives are aligned with this dynamic valuation. One way to achieve this is to embed time-coupled incentives directly into the smart contract. For example, the ransom schedule $R(t)$ can be specified to decline as $\delta(t)$ falls, which ensures that delaying the agreement strictly reduces the attacker's eventual payoff. Additional penalties for delay can also be introduced, such as gradually slashing the attacker's escrow balance or progressively shrinking the victim's refundable portion, so that both parties are better off finalizing the deal early rather than stalling. Furthermore, the attacker can be required to commit on-chain to a maximum negotiation horizon or to reveal the decryption key by a fixed deadline once certain conditions are satisfied, making any deliberate delay directly costly as $\delta(t)$ continues to drop.

*c) Mechanism Design Sketch:* **Dynamic valuation module.** The first component of the extended mechanism is a valuation module that formally defines $\delta(t)$, motivates a particular functional form using business-interruption cost models, and then derives how the cooperative surplus and Shapley allocations depend on time. This makes the impact of negotiation delays explicit in the underlying game.

**Dynamic smart contract.** Building on this module, a modified dual-deposit smart contract is specified in which the ransom due to the attacker is given by a function $R(t)$ directly linked to $\delta(t)$. The deposit and refund rules for both parties are chosen so that the unique rational strategy is to reach an agreement before $\delta(t)$ drops below a negotiated threshold, at which point further negotiation no longer creates meaningful surplus.

**Equilibrium analysis.** Finally, an equilibrium analysis is carried out to show that, under the proposed dynamic rules, the resulting fair ransom remains consistent with the current value $\delta(t)$ at every negotiation stage. At the same time, both attacker and victim retain incentives to participate only while there is positive surplus to share, which resolves the original static-$\delta$ limitation in Dilemma 2 and yields time-consistent "fair" ransom values.

## IV. Discussion & Future Work

While these modifications to Vakilinia et al.'s approach sufficiently address the highlighted research limitations, none of these solutions have been incorporated into a practical, enforceable framework that a victim could actually rely on during an attack. More research is needed on the practical implementation and replicability of the results to help validate or deny the effectiveness of the proposed ransomware negotiation mechanism design.

## V. Conclusion

Considering the lack of extensive ransomware negotiation models using smart-contracts, I have proposed modifications to a recent relevant paper to facilitate the negotiation between attacker and victim for the release of the decryption key. First, I have studied Vakilinia et al.'s 2021 Ransomware Mechanism Design approach, and then I have proposed significant modifications to the mechanism design for better applicability in real-life ransomware scenarios.

## References


[1] I. Vakilinia, M. M. Khalili, and M. Li, "A mechanism design approach to solve ransomware dilemmas," in *International Conference on Decision and Game Theory for Security*. Springer, 2021, pp. 181–194.

[2] C. Zhang and F. Luo, "Bargaining game theoretical analysis framework for ransomware attacks," *Journal of Information Security and Applications*, vol. 93, p. 104115, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212625001528

[3] H. Zhang, S. Shen, X. Hu, and C. Jin, "Ransomware negotiation: Dynamics and privacy-preserving mechanism design," 2025. [Online]. Available: https://arxiv.org/abs/2508.15844