A Quantitative Study across CIA (Confidentiality, Integrity, Availability) Triad and Performance in Blockchain-Based Crypto-Space

J. Seol
Computer Science
Middle Georgia State University
Macon, GA, USA
jongho.seol @mga.edu

J.Deuja
Computer Science
Oklahoma State University
Stillwater, OK, USA
jiwan.deuja@okstate.edu

Indy N. Park
Natural Science and Math
Vanguard University
Costa Mesa, CA, USA
indy.park@vanguard.edu

Cong Pu
Computer Science
Oklahoma State University
Stillwater, OK, USA
cong.pu@outlook.com

N. Park
Computer Science
Oklahoma State University
Stillwater, OK, USA
npark@cs.okstate.edu

***Abstract*—This paper presents a new quantitative model to study the interplay across CIA (Confidentiality, Integrity, Availability) Triad and performance in blockchain-based crypto space with specific reference to Ethereum or Ethereum-equivalent chains. The model introduces and incorporates three new random variables on top of the baseline chain model [16], C: the likelihood to secure confidentiality; I: to secure integrity; and A: to secure availability. Thus, the model will orchestrate an extensive set of key random variables such as λ: transaction slot arrival rate; μ: block posting rate; i: number of transaction slots pending on the current block along with C, I and A. The underlying mathematical method employed is an embedded Markovian queueing model as the model traces the stochastic flow of the transactions as well as the Markovian flow of them with respect to C, I and A. The state in the model is defined by $P_{i_{C/I/A}}$, i.e., the likelihood to have i number of transaction slots pending on the current block and the stochastic CIA status of the crypto space thus far is in C or $\overline{C}$, I or $\overline{I}$, and A or $\overline{A}$. The solutions to the model will be provided to assess a few basic performance metrics such as W : the average transaction waiting time, L: the average block capacity required; and G: the throughput of transactions per block. And further and primarily, a unique and extensive simulation and analysis will be conducted to evaluate the impact of base random variables such as i, λ, μ, and various combinations of C, I and A on the overall $P_{i_{C/I/A}}$ in steady state. The results of the simulation reveal tradeoffs between the CIA Triad and performance that is uniquely identifiable by the proposed model.**

Keywords—blockchain, confidentiality, integrity, availability

I. Introduction

Blockchain-based crypto-space is the known-best trustworthy network system by far [2-4]. Blockchain-based crypto-space theoretically guarantees its security as long as the 51% or more of the copies of blockchain distributed over the network are verified to be in agreement. Yet to come, there are pressing market demands and needs for further extensive and expansive orchestration of crypto-assets and resources across on- and off-chain (e.g., NFT, Non-Fungible Tokens [9,13]) and across heterogeneous chains (e.g., hybrid chain [14] and cross chain [13]). The security for off-chain assets in NFT chain and for assets in between hybrid (cross) chains are expected to be highly vulnerable to the potential security loopholes due to the intrinsically seamed nature of the transactions in those chains of concern.

It is presumed without loss of generality in this research that the biggest hurdle on the way against those demands are the potential vulnerability of the transactions to the security threats specifically concerning Confidentiality, Integrity, Availability (referred to as CIA Triad [1]) threats/risks and potential performance issues mainly due to the decentralized yet possibly seamed deployment of transactions across on- and off-chains [9,12] and across heterogeneous chains [13,14]. There has not been any adequate theory and practice in place to address and assure the vulnerability. CIA Triad has been addressed in qualitative manners [5-8] but has never been quantitatively addressed and researched adequately in the particular context of concern in crypto-space, to the best of the PI's knowledge.

In this context, this research will investigate how to establish a theoretical foundation to model and assure across CIA triad and performance in blockchain-based crypto space in a quantitative manner. The CIA triad will be addressed and incorporated on top of the baseline chain model [16]. The baseline chain model assumes a blockchain-based crypto-space under ideal circumstance without any potential threats/risks to CIA triad and the due potential performance loss. In practice, CIA triad and performance are under a constraint to be sentenced by, namely, the Grand Budget, such that either to identify an optimal CIA triad budget allocation under a performance constraint, or vice versa. In this research, an emphasis will be given on the CIA triad tracing under performance constraints, namely, and which will serve as the central and primary figure of merit to be quantitatively defined as the likelihood to have i

number of slots of transactions in a block in a normalized manner with all C, I and A being secured under performance constraint, and to be expressed by $P_{i,CIA}$.

Extensive numerical simulations will be conducted to validate the efficacy of the proposed model with respect to various design variables such as i, λ, μ, and various combinations of C, I and A versus the overall $P_{i_{C/I/A}}$ in steady state.

This paper is organized as follows: preliminary works will be presented and reviewed in the following section; the proposed model and its solution will be presented in the next section; then extensive numerical simulations and analysis will be provided; lastly, conclusions and discussion section will be presented.

II. Preliminaries and Literature Review

The baseline chain model [16] is employed and serves as an ideal blockchain-based crypto-space such that it assumes no threats on CIA, i.e., $C = I = A = 100\%$ (or 0 tpm, threats per million accesses), and no assumptions are made in regard of performance optimization other than baseline, in order to reveal the bare CIA status along with performance without any optimization efforts attempted.

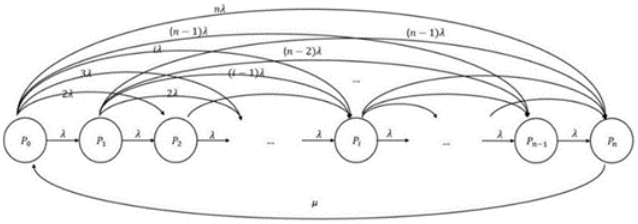

Figure 1. Baseline chain model diagram.

The underlying blockchain-based crypto-space will assume a Proof-of-Work and ERC20-based Ethereum network system. The proposed CIA-Driven Blockchain-Based Crypto-Space Model will be built on top of the Baseline Chain Model as shown in the Figure 1 above [16]. The primary variables in the baseline model are the number of slots ($0 \leq i \leq n$) such that each transaction will be tracked as a sequence of slots being executed in the course of the block-wise operation of mining and block-posting, along with the transactions arrival rate and block-posting rates. On top of the baseline model, C, I and A variables will be incorporated such that CIA (i.e., a series product of C, I and A) represents the likelihood for the current transaction to be checkpointed for all the three CIA requirements, (i.e., the transaction being executed currently is checkpointed to be perfectly secure and trustworthy in other words); $CI\bar{A}$ the likelihood to be checkpointed for C and I requirements yet the crypto-space is not available, i.e., $\bar{A}$; $C\bar{I}$ the likelihood only C requirement is checkpointed but the crypto-space has been altered in a maliciously-minded manner, i.e., $\bar{I}$, and note that in this case once the crypto-space has been altered it is assumed that there is no further consideration on the A requirement; and lastly $\bar{C}$ the likelihood not to be checkpointed for any of those CIA requirements, and note that if C requirement has been checkpointed to be violated, then there is no further consideration on any other requirements. Also, note that the model can be extended to take rollback steps (i.e., the steps to restore the CIA status back to the most recent checkpoint) can be taken into account.

The baseline model has been solved in a previous work as reported in [16], where P_i, i.e., the likelihood that the i_{th} transaction has been mined and is being executed to be posted in the current block, has been solved as follows.

$$P_i = \frac{2}{(n-i)(n-i+1)} P_0 \left(\left(\frac{i(i+1)}{2} \right) \frac{n}{\left(\sqrt{2\pi n} \left(\frac{n}{e} \right)^n \right)^2} (2^{i-1}(in - 2n + 7i - 14 - i^2) + 8) + i \right)$$

where n is the maximum number of slots a block can accommodate unless otherwise controlled, and $0 \leq i \leq n$.

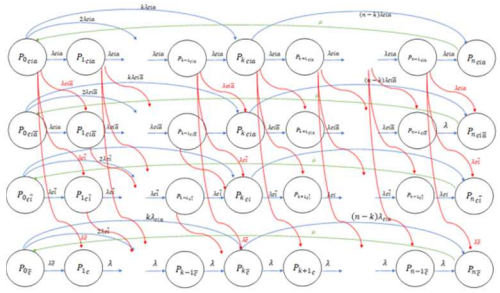

Figure 2. CIA Triad model configuration.

A new quantitative model is proposed in this research to express and assure the CIA Triad status of blockchain-based crypto-space. The quantitative model will be built of three primary security-specific base variables as defined as follows: C (Confidentiality): likelihood (%) to protect information from unauthorized access and misuse during the transaction currently being executed; I (Integrity): likelihood to protect information from unauthorized alteration; and A (Availability): likelihood to protect timely and uninterrupted access to the system.

The underlying blockchain-based crypto-space will assume an Ethereum network system. The model will be built on top of the baseline model specific to the underlying crypto-space. The primary variables in the baseline model will be the number of slots ($0 \leq k \leq n$) such that each transaction will be tracked as a sequence of slots being executed in the course of the block-wise operation of mining and block-posting, along with the transactions arrival rate and block-posting rates. On top of the baseline model, C, I and A variables will be incorporated such that CIA (i.e., a series product of C, I and A) represents the likelihood for the current transaction to be checkpointed for all the three CIA requirements, (i.e., the transaction being executed currently is checkpointed to be perfectly secure and trustworthy in other words); $CI\bar{A}$ the likelihood to be checkpointed for C and I requirements yet the crypto-space is not available, i.e., $\bar{A}$; $C\bar{I}$ the likelihood only C requirement is checkpointed but the crypto-space has been altered in a maliciously-minded manner, i.e., $\bar{I}$, and note that in this case once the crypto-space has been altered there is no need for further consideration on the A requirement; and lastly $\bar{C}$ the likelihood not to be checkpointed

for any of those CIA requirements, and note that if C requirement has been checkpointed to be violated, then there is no need for any further consideration on any other requirements. Also, note that the model can be extended to take rollback steps (i.e., the steps to restore the CIA status back to the most recent checkpoint) can be taken into account.

III. Proposed CIA Chain Model

A new quantitative model is proposed in this research to express and assure the CIA Triad status of blockchain-based crypto-space. The quantitative model will be built of three primary security-specific base variables as defined as follows: C (Confidentiality): likelihood (%) to protect information from unauthorized access and misuse during the transaction currently being executed; I (Integrity): likelihood to protect information from unauthorized alteration; and A (Availability): likelihood to protect timely and uninterrupted access to the system.

The underlying blockchain-based crypto-space will assume an Ethereum network system. The model will be built on top of the baseline model specific to the underlying crypto-space. The primary variables in the baseline model will be the number of slots ($0 \leq k \leq n$) such that each transaction will be tracked as a sequence of slots being executed in the course of the block-wise operation of mining and block-posting, along with the transactions arrival rate and block-posting rates. On top of the baseline model, $C, I,$ and A variables will be incorporated such that CIA (i.e., a series product of $C, I,$ and A) represents the likelihood for the current transaction to be checkpointed for all the three CIA requirements, (i.e., the transaction being executed currently is checkpointed to be perfectly secure and trustworthy in other words); $CI\bar{A}$ the likelihood to be checkpointed for C and I requirements yet the crypto-space is not available, i.e., $\bar{A}$; $C\bar{I}$ the likelihood only C requirement is checkpointed but the crypto-space has been altered in a maliciously-minded manner, i.e., $\bar{I}$, and note that in this case once the crypto-space has been altered there is no need for further consideration on the A requirement; and lastly $\bar{C}$ the likelihood not to be checkpointed for any of those CIA requirements, and note that if C requirement has been checkpointed to be violated, then there is no need for any further consideration on any other requirements. Also, note that the model can be extended to take rollback steps (i.e., the steps to restore the CIA status back to the most recent checkpoint) can be taken into account.

Based on the variables as defined in the baseline model, a new Embedded Markovian Queueing Model is proposed as shown in the Figure 1. The state of the crypto-space will be defined as in the baseline model, i.e., the number of slots of each transaction being currently executed (in order to demonstrate the model tracks the unique blockchain-specific stochastic flow of transactions), and the state transition rates will be defined such that the number of slots (i) per transaction be in 4 different states, namely, $P_{i_{CIA}}$, $P_{i_{CI\bar{A}}}$, $P_{i_{C\bar{I}}}$, and $P_{i_{\bar{C}}}$. The balance equations for the CIA Triad Model with checkpoint (i.e., each concluded state will be considered as a checkpoint state if a rollback step is assumed to be in place) but without a rollback taken into account are shown as follows (to be solved in the proposed research in a form as closed as possible, which might involve mathematical approximations wherever there is no known mathematical solutions available).

$$P_{n_{CIA}} = CIA\frac{\lambda}{\mu}\frac{n(n+1)}{2}P_{0_{CIA}}$$

$$P_{i_{CIA}} = q_{i_{CIA}}P_{0_{CIA}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CIA}}\right]k\right]+i\right]$$

where,

$0 < i < n$

$$q_{l_{CIA}} = \frac{2}{(n-i)(n-i+1)}(CIA + CI\bar{A} + C\bar{I} + \bar{C})^{-1}CIA$$

$$P_{n_{CI\bar{A}}} = CI\bar{A}\frac{\lambda}{\mu}\frac{n(n+1)}{2}\left(P_{0_{CI\bar{A}}} - P_{0_{CIA}}\right)$$

$$P_{i_{CI\bar{A}}} = q_{i_{CIA}}P_{0_{CIA}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CIA}}\right]k\right]+i\right] + q_{i_{CI\bar{A}}}P_{0_{CI\bar{A}}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CI\bar{A}}}\right]k\right]+i\right]$$

where, $0 < i < n$, and

$$q_{i_{CI\bar{A}}} = \frac{2}{(n-i)(n-i+1)}(CI\bar{A} + C\bar{I} + \bar{C})^{-1}CI\bar{A}$$

$$q_{i_{CIA}} = \frac{2}{(n-i)(n-i+1)}(CIA + CI\bar{A} + C\bar{I} + \bar{C})^{-1}CIA$$

$$P_{n_{C\bar{I}}} = C\bar{I}\frac{\lambda}{\mu}\frac{n(n+1)}{2}\left(P_{0_{C\bar{I}}} - P_{0_{CI\bar{A}}}\right)$$

$$P_{i_{C\bar{I}}} = q_i P_{0_{CIA}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CIA}}\right]k\right]+i\right] + q_i P_{0_{CI\bar{A}}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CI\bar{A}}}\right]k\right]+i\right] + q_i P_{0_{C\bar{I}}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{C\bar{I}}}\right]k\right]+i\right]$$

where, $0 < i < n$, and

$$q_{i_{C\bar{I}}} = \frac{2}{(n-i)(n-i+1)}(C\bar{I} + \bar{C})^{-1}C\bar{I}$$

$$q_{i_{CI\bar{A}}} = \frac{2}{(n-i)(n-i+1)}(CI\bar{A} + C\bar{I} + \bar{C})^{-1}CI\bar{A}$$

$$q_{i_{CIA}} = \frac{2}{(n-i)(n-i+1)}(CIA + CI\bar{A} + C\bar{I} + \bar{C})^{-1}CIA$$

$$P_{n_{\bar{C}}} = \bar{C}\frac{\lambda}{\mu}\frac{n(n+1)}{2}\left(P_{0_{\bar{C}}} - P_{0_{C\bar{I}}}\right)$$

$$P_{i_{\bar{C}}} = q_{i_{CIA}}P_{0_{CIA}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CIA}}\right]k\right] + i\right] + q_{i_{CI\bar{A}}}P_{0_{CI\bar{A}}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{CI\bar{A}}}\right]k\right] + i\right] + q_{i_{C\bar{I}}}P_{0_{C\bar{I}}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{C\bar{I}}}\right]k\right] + i\right] + q_{i_{\bar{C}}}P_{0_{\bar{C}}}\left[\sum_{j=1}^{i} j\left[\sum_{k=1}^{i-1}\left[\prod_{l=1}^{k-1} q_{l_{\bar{C}}}\right]k\right] + i\right]$$

where, $0 < i < n$, and

$$q_{i_{\bar{C}}} = \frac{2}{(n-i)(n-i+1)}(\bar{C})^{-1}\bar{C} = \frac{2}{(n-i)(n-i+1)}$$

$$q_{i_{C\bar{I}}} = \frac{2}{(n-i)(n-i+1)}(C\bar{I} + \bar{C})^{-1}C\bar{I}$$

$$q_{i_{CI\bar{A}}} = \frac{2}{(n-i)(n-i+1)}(CI\bar{A} + C\bar{I} + \bar{C})^{-1}CI\bar{A}$$

$$q_{i_{CIA}} = \frac{2}{(n-i)(n-i+1)}(CIA + CI\bar{A} + C\bar{I} + \bar{C})^{-1}CIA$$

IV. Numerical Simulation Results and Analysis

Through the utilization of simulation results, we validate the previously introduced CIA (Confidentiality, Integrity and Availability Triad) state within the blockchain-based crypto space by scrutinizing variations in properties such as W, the average transaction slot waiting time, L, the average block size, G (γ), the throughput of transactions per block, and the concerning changes in λ, μ, and CIA. The simulation underscores the inherent challenge of maintaining high confidentiality, primarily attributed to the transparent nature of transaction data. Integrity, on the other hand, is rigorously maintained through strategic measures such as data signing, hash chaining, and consensus protocols, effectively thwarting unauthorized alterations [19,20]. The distributed architecture ensures a robust level of availability, assuring swift and uninterrupted system access through the replication of blockchain across nodes [21-23]. Security aspects can be quantified, encompassing variables such as the threats to confidentiality via unauthorized access, the threats to integrity via changeability, and the threats to the availability via system downtime. Visual representations, including plotted graphs elucidating trends in the interplay between the performance and system's CIA triad status, serve to articulate the dynamic nature of system confidentiality, integrity and availability versus the performance. The overarching aim is to provide a concise yet comprehensive overview of the blockchain system's performance trends in adhering to the principles of the CIA Triad.

Figures 3 and 4 depict the relationship between W and n under varying levels of CIA (low confidentiality, medium Integrity, and high Availability), with Figure 1 spotlighting the impact of the crucial variable λ across the assumed CIA ranges. Notably, as λ decreases under given CIA in Figure 1, W elevates significantly, contrasting with the lowest values observed when λ is high. Likewise, Figure 2 illustrates the relationship between W and n under various λ levels and CIA (high confidentiality: 1,000 in threats per million (tpm), medium Integrity: 100, and low Availability: 1), showcasing patterns comparable to Figure 1. However, Figure 2 initiates with a notably higher W value at n =0 compared to Figure 1. These visualizations provide valuable insights into the intricate interplay of $W, n,$ λ, and CIA levels, elucidating how changes in these variables influence the observed patterns.

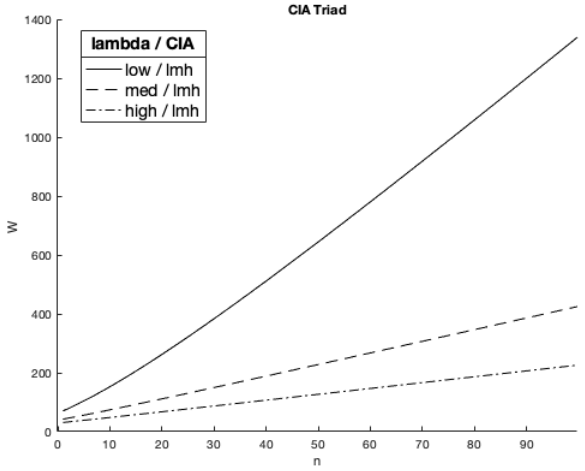

Figure 3. W vs. n and CIA_{lmh}

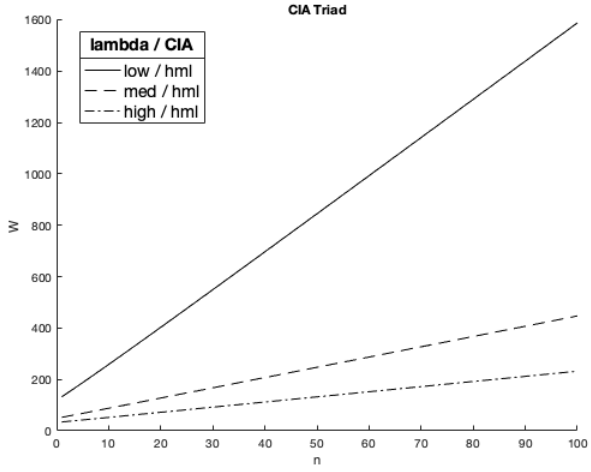

Figure 4. W vs. n and CIA_{hml}

Figures 5 and 6 present a comprehensive analysis of the dynamic interplay between L and n, considering fluctuations in λ (low, medium, high) and CIA levels (low, medium, high) and vice versa. Specifically, Figure 3 unfolds the relationship by plotting the value of W against n, aligning with the observed pattern in Figure 1. Figure 4 introduces three distinct functions, deviating from those in Figures 1 and 2, marked by varying constants. Scrutinizing these figures yields valuable insights into the distinctive features of the CIA triad model. A notable distinction emerges between Figure 3 and Figure 4 in terms of CIA levels—arranged as low, medium, and high in Figure 3, and high, medium, and low in Figure 4. This discrepancy significantly influences the L value manifesting the lowest values for low λ with high, medium, and low CIA levels and the highest values for high λ with high, medium, and low CIA levels. Thus, the analytical findings underscore the pivotal role of the CIA triad model, indicating that alterations in the CIA levels from low, medium, and high to high, medium, and low lead to nuanced outcomes based on the inherent characteristics of the model.

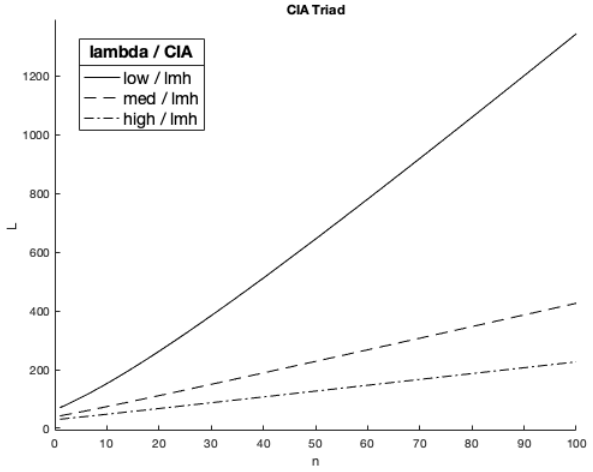

Figure 5. L vs. n and CIA_{lmh}

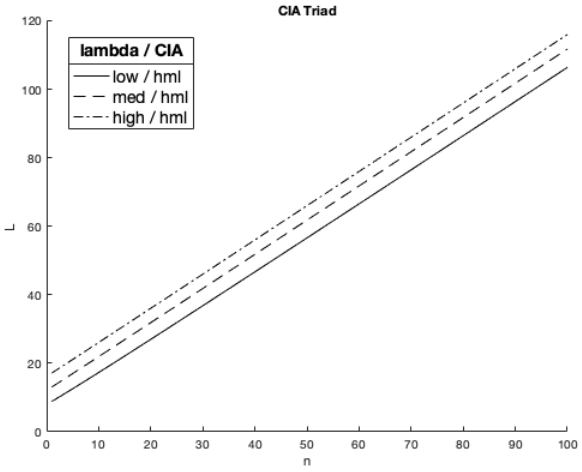

Figure 6. L vs. n and CIA_{hml}

Figures 7 and 8 elucidate the relationship between G (γ) values and n, exploring variations in λ (low, medium, high) alongside CIA levels (low, medium, high), and vice versa. The results underscore the performance of the CIA triad model, revealing that γ values peak when λ is at its highest, regardless of CIA levels, and vice versa. Upon closer scrutiny, the patterns in both figures exhibit similarities, emphasizing a pronounced impact on performance with high, medium, and low CIA levels. Specifically, G values initiate at 0.055, 0.045, and 0.025 for CIA levels low, medium, and high, respectively, and commence at 0.064, 0.062, and 0.052 for CIA levels high, medium, and low, respectively. This analysis reveals that the CIA triad model excels under conditions of high, medium, and low CIA levels. Notably, the G value of λ-low and CIA -high, medium, and low (0.052) represents the lowest performance point, slightly below the highest G value (0.055) of the CIA low, medium, and high model. In essence, this indicates that the CIA triad model exhibits superior performance, particularly under high, medium, and high CIA conditions.

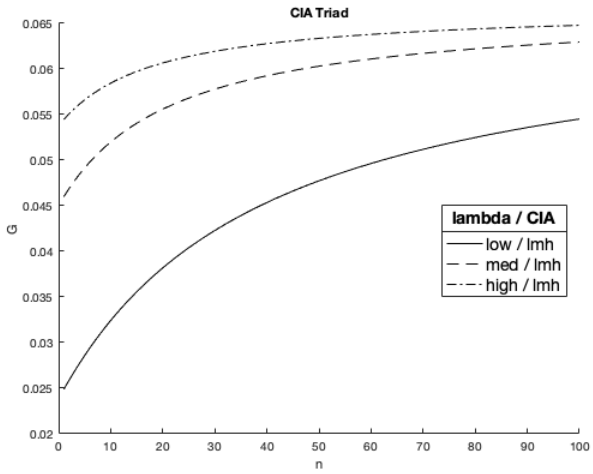

Figure 7. G vs. n and CIA_{lmh}

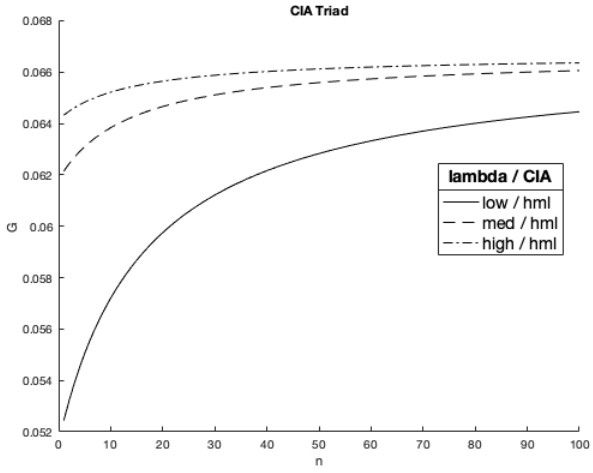

Figure 8. G vs. n and CIA_{hml}

Figures 9 through 16 illustrate the steady-state probability for the current and preceding blocks, encompassing confidentiality, integrity protection breach, and availability in the foundational CIA model. Specifically, Figures 7 and 8 portray the steady state probability, $P_{i_{CIA}}$, values against n, considering variations in λ (low, medium, high) and CIA levels (low, medium, high), and vice versa. Notably, Figure 7 exhibits slightly lower $P_{i_{CIA}}$ values than Figure 8, with both figures indicating that P values reach their peak when λ is high, regardless of CIA levels, and vice versa.

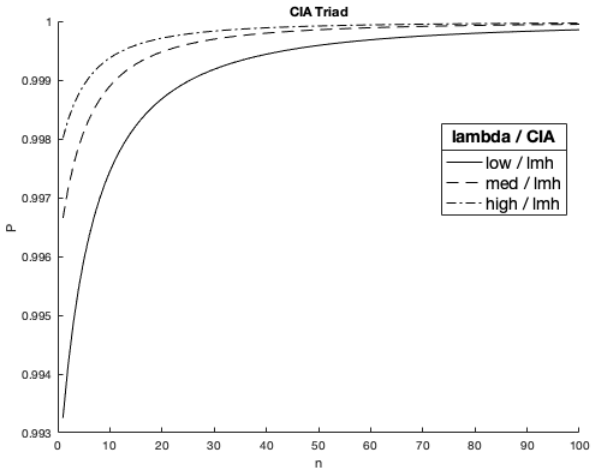

Figure 9. $P_{i_{CIA}}$ vs. n and CIA_{lmh}

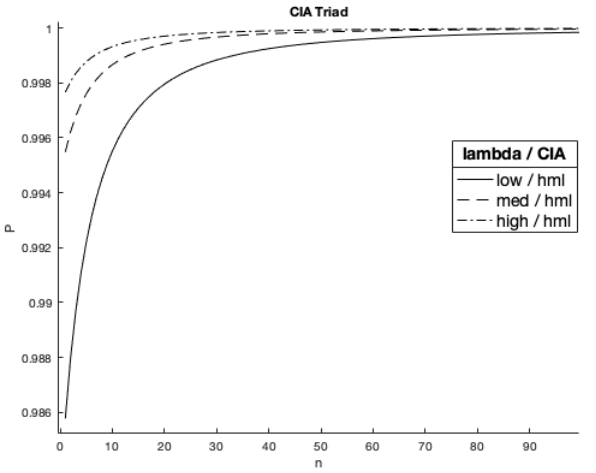

Figure 10. $P_{i_{CIA}}$ vs. n and CIA_{hml}

Moving on to Figures 11 and 13, they depict $P_{i_{CI\bar{A}}}$ at varying λ and CIA levels, while Figures 13 and 14 showcase $P_{i_{C\bar{I}}}$ and Figures 15 and 16 display $P_{i_{\bar{C}}}$ all under similar conditions. Remarkably, the patterns across Figures 9 to 14 appear quite similar within each pair (e.g., 11 and 12, 13 and 14, 15 and 16), irrespective of CIA levels. This similarity persists even when transitioning between CIA levels (low, medium, high) and vice versa. Notably, the consistency in patterns across these figures underscores the convergence of $P_{i_{\bar{C}}}$ values within each pair when delving into the CIA model, emphasizing a uniformity in the observed values.

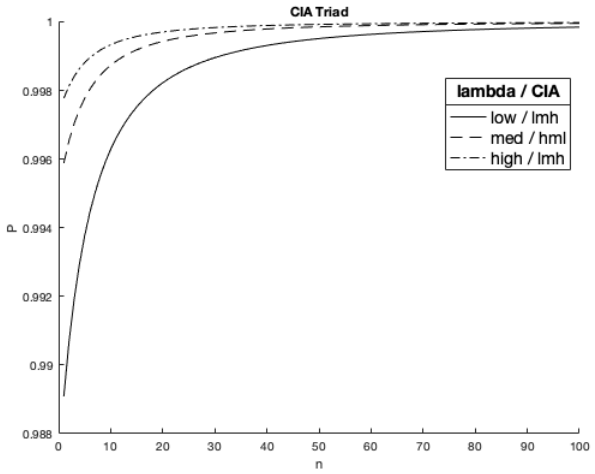

Figure 11. $P_{i_{CI\bar{A}}}$ vs. n, CIA_{lmh}

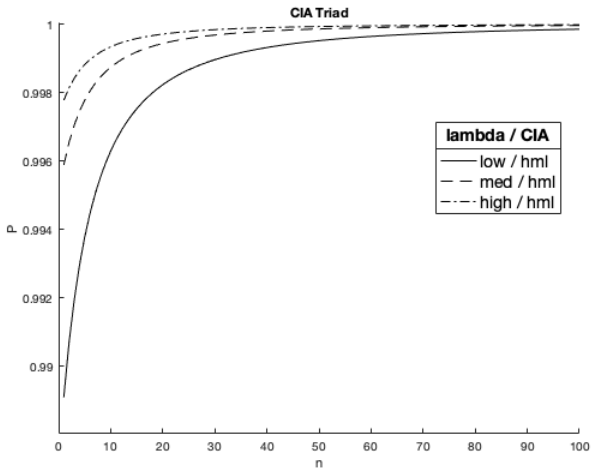

Figure 12. $P_{i_{CI\bar{A}}}$ vs. n, CIA_{hml}

In this comprehensive analysis of the blockchain-based crypto space, a quantitative model is validated through simulation results, assessing properties (W, L, G, P) in response to variations in λ, μ, and the CIA, and is summarized as follows.

Figures 5 and 6 delved into the dynamic relationship between L and n, revealing insights into the distinctive features of the triad model. Notably, the arrangement of CIA levels played a significant role in influencing L values. Figures 5 and 6 explored γ values, demonstrating the model's superior performance under high, medium, and low CIA conditions. The consistency in patterns across these figures suggests a uniform convergence of performance values within each pair.

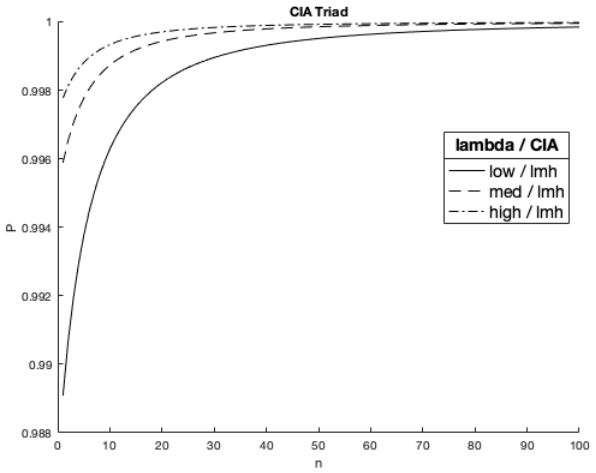

Figure 13. $P_{i_{C\bar{I}}}$ vs. n, CIA_{lmh}

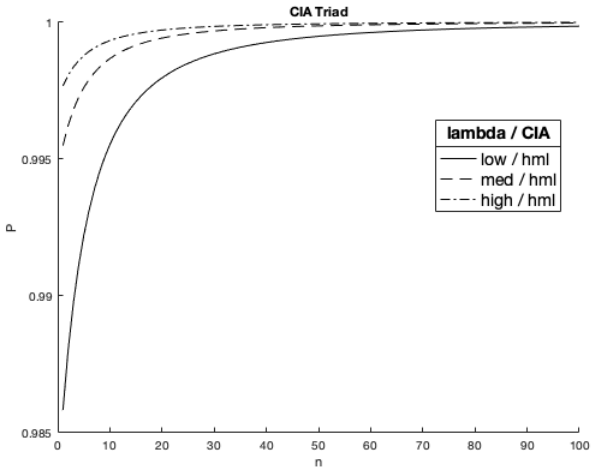

Figure 14. $P_{i_{C\bar{I}}}$ vs. n, CIA_{hml}

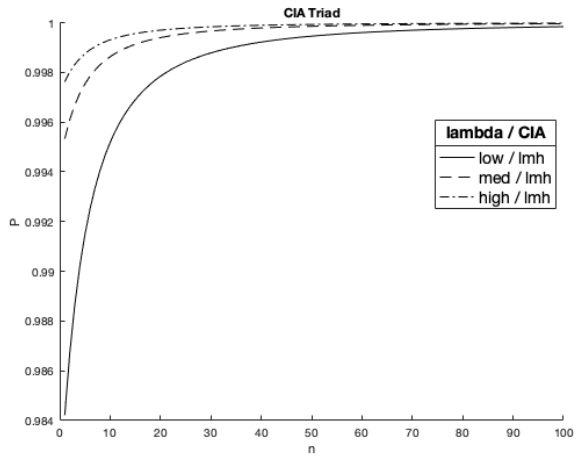

Figure 15. $P_{i_{\bar{C}}}$ vs. n, CIA_{lmh}

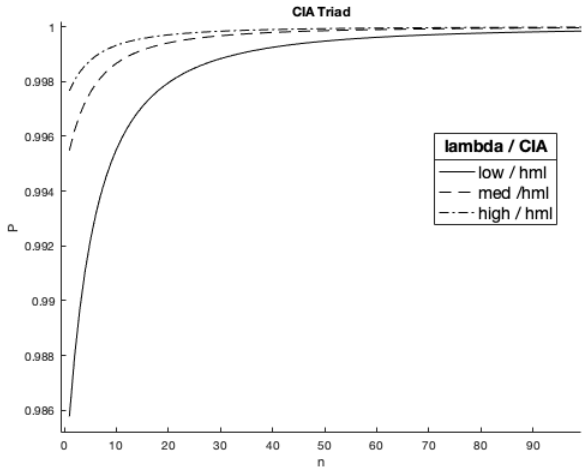

Figure 16. $P_{i_{\bar{C}}}$ vs. n, CIA_{hml}

Finally, Figures 9 through 16 provided a comprehensive illustration of steady-state probabilities for i number of transaction slots pending on the block under a certain CIA triad status, e.g., $P_{i_{CIA}}$, $P_{i_{CI\bar{A}}}$, $P_{i_{C\bar{I}}}$ and $P_{i_{\bar{C}}}$. Noteworthy were the slightly lower $P_{i_{CIA}}$ values in Figure 7 compared to Figure 8, with both indicating peak values when λ was high, regardless of CIA levels. The subsequent figures exhibited similar patterns within each pair, emphasizing a convergence of $P_{i_{CI\bar{A}}}$, $P_{i_{C\bar{I}}}$ and $P_{i_{\bar{C}}}$ values when transitioning between CIA levels. Overall, this detailed analysis demonstrates the performance trends of the blockchain-based crypto system under the given principles of the CIA Triad.

Some of the noteworthy simulation results are highlighted as follows.

Quantification of Security Aspects: The analysis quantifies various security aspects, including unauthorized access (i.e., confidentiality), changeability (i.e., integrity), and system downtime (i.e., availability). This provides a detailed understanding of the vulnerabilities and strengths within the blockchain system concerning these security dimensions.

Influence of λ and CIA Levels on Performance: Figures 1 and 2 highlighted the intricate interplay of variables ($W, n,$ λ, and CIA levels), indicating patterns influenced by changes in these variables. The arrangement of CIA levels significantly impacted L values in Figures 5 and 6, shedding light on the nuanced outcomes based on the inherent characteristics of the CIA triad model.

Superior Performance under Certain CIA Conditions: Figures 7 and 8 reveals the superior performance of the CIA triad model, particularly under conditions of high (1000), medium (100) , and low (1) CIA levels. The consistency in patterns across these figures indicates a convergence of performance values within each pair.

Steady-State Probabilities and CIA Model Convergence: Figures 9 through 16 provides a comprehensive illustration of steady-state probabilities for $P_{i_{CIA}}$, $P_{i_{CI\bar{A}}}$, $P_{i_{C\bar{I}}}$ and $P_{i_{\bar{C}}}$. It is noteworthy that the slight differences in $P_{i_{CIA}}$ values between

Figure 9 and Figure 10 and the consistent patterns within each pair suggested a convergence of the steady-state probabilities when transitioning between CIA levels.

In summary, the findings underscore the complex dynamics of the blockchain system in adhering to the principles of the CIA Triad, offering insights into the trade-offs and strengths associated with confidentiality, integrity, and availability in the context of blockchain-based transactions.

V. Conclusion and Discussions

This paper has presented a quantitative model to evaluate the interplay across CIA (Confidentiality, Integrity, Availability) Triad and performance in blockchain-based crypto space employing an embedded Markovian queueing model method, and Ethereum or Ethereum-equivalent chains have been under consideration. The model is based on the baseline chain model [16] and incorporates three new random variables on top of, C: confidentiality; I: integrity; and A: availability, in addition to λ, μ, i. The model traces the stochastic flow of the transactions as well as the Markovian flow of them with respect to C, I and A. The model is centered around $P_{i_{C/I/A}}$. The solutions to the model have been provided to assess a few basic performance metrics such as W, L ,and $G,$ and primarily, a unique and extensive simulation and analysis have been conducted to evaluate the impact of base random variables such as i, λ, μ, and various combinations of C, I and A on the overall $P_{i_{C/I/A}}$ in steady state. Quantification of Security Aspects: The analysis quantifies various security aspects, including unauthorized access (i.e., confidentiality), changeability (i.e., integrity), and system downtime (i.e., availability). This provides a detailed understanding of the vulnerabilities and strengths within the blockchain system concerning these security dimensions. The study has intricately examines the dynamic interplay among variables, including W, n, λ and levels of the CIA (Confidentiality, Integrity, Availability) triad. It has been observed that the configuration of CIA levels notably influences L values, illuminating nuanced outcomes linked to the inherent characteristics of the CIA triad model. The results of the simulation reveal tradeoffs between the CIA Triad and performance that is uniquely identifiable by the proposed model. Ultimately the work presented in this paper will provide a theoretical yet practically agreeable foundation to designing an optimal CIA Triad-aware blockchain-based crypto space under given performance, or vice versa.

[1] Jeroen Van Der Ham,‘’Toward a Better Understanding of “Cybersecurity”’’, Digital Threats: Research and PracticeVolume 2Issue 3Article No.: 18pp 1–3

[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf

[3] Gavin Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger, Petersburg Version 4ea7b96 – 2020-06-08”, Yellow Paper, Jun 8 2020

[4] Vitalik Buterin, “A Next Generation Smart Contract & Decentralized Application Platform”, White Paper, 2014.

[5] Federico Lombardi, Leonardo Aniello, Stefano De Angelis, Andrea Margheri, and Vladimiro Sassone, “A Blockchain-based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids”, Living in the Internet of Things: Cybersecurity of the IoT – 2018. DOI: 10.1049/cp.2018.0042

[6] Keke Gai, Yulu Wu, Liehuang Zhu, Zijian Zhang, and Meikang Qiu, “Differential Privacy-Based Blockchain for Industrial Internet-of-Things”, IEEE Transactions on Industrial Informatics (Volume: 16, Issue: 6, June 2020). DOI: 10.1109/TII.2019.2948094

[7] Keke Gai, Yulu Wu, Liehuang Zhu, Meikang Qiu, and Meng Shen, "Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid”, IEEE Transactions on Industrial Informatics (Volume: 15, Issue: 6, June 2019). DOI: 10.1109/TII.2019.2893433

[8] Keke Gai, Yulu Wu, Liehuang Zhu, Lei Xu, and Yan Zhang, “Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks", IEEE Internet of Things Journal (Vomue:6, Issue:5, Oct 2019). DOI: 10.1109/JIOT.2019.2904303

[9] K. Kentner, J. Seol and N. Park, "A Real-Time Performance Model for NFT Chains", IEEE BCCA, October, 2023

[10] J. Seol, K. Kentner, Indy N. Park, S. Joshi and N. Park, "An Adaptive Blockchain-based Decentralized Network Computing and Performance Analysis", IEEE BCCA, October, 2023

[11] J. Seol and N. Park,"An Asynchronous Chain and A Variable Bulk Arrival and Asynchronous Bulk Service Model", ACM BSCI, July, 2023

[12] J. Seol, J. Ke, A. Kancharla, S. Joshi and N. Park, "A Bivariate Performance Model across On- and Off-Chain in A NFT (Non-Fungible Token) Chain", IEEE BCCA 2022

[13] J. Ke, J. Seol, A. Kancharla and N. Park, "Performance Modeling and Assurance for Cross Chain", IEEE BCCA 2022

[14] A. Kancharla, J. Seol, N.-J. Park, T. Feng and N. Park, "A Hybrid Chain and A Variable Bulk Arrival and Static Bulk Service of Double-Tuple Queueing Model", IEEE ICBC 2021 (poster)

[15] A. Kancharla, J. Seol, H.-Y. Kim and N. Park, "Distributed Decentralized Chain (DDC) and k-Queue Variable Bulk Arrival and Static Bulk Service model", ACM BSCI 2021

[16] J. Seol, A. Kancharla and Z. Ke and N. Park, "A Variable Bulk Arrival and Static Bulk Service Model for Blockchain", ACM BSCI 2020

[17] Abhilash Kancharla, Indy Park, Nicole Park and N. Park, "Dependable Industrial Crypto Computing", IEEE ISIE 2019

[18] Abhilash Kancharla and N. Park, "Slim Chain and Dependability", ACM BSCI 2020

[19] Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). Blockchain-based database to ensure data integrity in cloud computing environments.

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

[21] Aviv, I., Barger, A., Kofman, A., & Weisfeld, R. (2023). Reference Architecture for Blockchain-Native Distributed Information System. *IEEE Access*, *11*, 4838-4851.

[22] Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310, No. 4, pp. 1-4).

[23] Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications* (pp. 1-307). Cham: Springer.