DOI: 10.5281/zenodo.21068513 **Volume 1 | Issue 1 | ISSN: 3141-643X | Published: 2026**

Ktrend - International Journal of Computer Science and Artificial Intelligence (IJCSAI)

A Hybrid Deterministic Mathematical Model for Secure Blockchain Transaction Dynamics Incorporating Lattice-Based Cryptography and Algebraic Semigroup Reconstruction

Utomobong M. Okon

Department of Mathematics, Akwa Ibom State University, Nigeria

Email: utomobongokon@gmail.com

Abstract

The security of blockchain transactions depends on the ability of a distributed ledger to maintain integrity, resist adversarial manipulation, and recover from compromised validation states. This paper develops a hybrid deterministic mathematical model for blockchain transaction security by combining lattice-based cryptographic protection with algebraic semigroup reconstruction. The model classifies active transaction units into secure, vulnerable, compromised, and recovered states. A nonlinear system of ordinary differential equations is derived to represent attack interaction, vulnerability progression, cryptographic protection, ordinary recovery, and semigroup-based reconstruction. The resulting model is shown to be positive, bounded, and mathematically well posed in a feasible region. An attack-free equilibrium and a compromised-state equilibrium are obtained. Using the next-generation matrix method, a blockchain security threshold $\mathcal{R}_s$ is derived. The attack-free equilibrium is locally asymptotically stable whenever $\mathcal{R}_s < 1$ and unstable whenever $\mathcal{R}_s > 1$. Numerical simulations show that increasing the lattice protection coefficient and the semigroup reconstruction efficiency lowers the persistence of compromised transactions and increases system resilience. Sensitivity analysis indicates that the attack interaction coefficient and vulnerability progression rate increase attack persistence, whereas lattice protection, recovery, and semigroup reconstruction reduce it. The study provides a rigorous modelling framework for analysing blockchain security in post-quantum and algebraic computational environments.

Keywords: deterministic modelling; blockchain security; lattice-based cryptography; semigroup reconstruction; stability analysis; numerical simulation; algebraic cryptography.

1. Introduction

Blockchain systems are built on sequential validation, cryptographic authentication, and distributed agreement. A transaction becomes useful only after it passes through a sequence of transformations: creation, propagation, validation, block inclusion, and confirmation. This sequential structure gives blockchain a natural algebraic interpretation because transaction states can be represented as transformations acting on a finite or countable state space. Recent work on differential semigroups of automaton perturbations and incremental syntactic reconstruction provides a useful foundation for modelling state transitions in systems where small perturbations may change the resulting computational language or validation pathway [1]. A related categorical approach to syntactic semigroups and language transformations supports the interpretation of blockchain validation as a composition of structured transition maps [2].

The algebraic security of digital systems is closely connected to the structure of finite groups, semigroups, lattices, homomorphisms, and computational invariants. Algorithms for modular isomorphism in small group orders illustrate how structural recognition problems can be treated computationally [3]. Enveloping semigroups in transformation groups also provide an algebraic and topological basis for analysing state evolution, proximal equivalence, and homomorphic images [4]. These ideas are relevant to blockchain because compromised transactions may be interpreted as perturbed states, while recovery may be viewed as a reconstruction process over a transformation system.

Classical finite algebra also motivates the present work. The classification of finite linear groups, Hall classes, nilpotency, modular subnormality, B-algebras generated by modulo integer groups, and homomorphism enumeration all provide useful structural tools for modelling algebraic state spaces [5, 6, 7, 8]. In cryptographic systems, lattice methods have become important because they provide strong candidates for post-quantum security. Lattice-based schemes have already been applied to secure blockchain development and financial systems [9]. The teaching and communication of abstract algebraic structures also remain important because applied models of this type depend on clear understanding of groups, subgroups, semigroups, and related finite structures [10]. Numerical modelling experience from nonlinear differential equations also supports the use of deterministic simulation in analysing the behaviour of nonlinear systems [11].

The present study develops a deterministic security model for blockchain transaction dynamics. It introduces two central parameters: a lattice protection coefficient, which measures the ability of lattice-based cryptography to prevent vulnerable transactions from becoming compromised, and a semigroup reconstruction coefficient, which measures the ability of algebraic transformation rules to reconstruct compromised states. The model is not designed to replace cryptographic proof systems. Instead, it gives a mathematical framework for studying the macro-level behaviour of secure, vulnerable, compromised, and recovered transaction classes.

1.1. Motivation

The motivation for this paper is threefold. First, modern blockchain systems require security models that can incorporate post-quantum cryptographic mechanisms. Second, blockchain transaction states evolve through sequential transformations, making semigroup methods natural tools for describing state evolution. Third, many digital financial systems operate in socioeconomic environments where transaction security has direct implications for business confidence, currency stability, and financial inclusion [12]. Algebraic invariants such as Ulm functions also motivate the use of structural descriptors when analysing transitivity and state transformation in algebraic systems [13]. Therefore, a hybrid mathematical model combining cryptographic strength and algebraic reconstruction can provide insight into the conditions under which compromised transaction activity dies out.

1.2. Main contributions

The main contributions of this paper are as follows:

(i) A deterministic blockchain security model is formulated using secure, vulnerable, compromised, and recovered transaction states.

(ii) Lattice-based cryptographic protection and algebraic semigroup reconstruction are incorporated as explicit model parameters.

(iii) Positivity, boundedness, and invariance of the feasible solution region are established.

(iv) A blockchain security threshold $\mathcal{R}_s$ is derived using the next-generation matrix approach.

(v) Local stability of the attack-free equilibrium is analysed.

(vi) Numerical simulations and sensitivity indices are used to show how protection and reconstruction influence security outcomes.

2. Mathematical Background and Related Work

A blockchain ledger can be viewed as a discrete dynamical system in which transaction states evolve under validation maps. If X denotes a set of transaction states and $T : X \to X$ denotes a validation map, then repeated validation produces a sequence $x, T(x), T^2(x), \ldots$. A family of such maps that is closed under composition forms a transformation semigroup. Semigroup methods are therefore suitable for modelling blockchain state evolution, especially when compromised states are treated as perturbations of valid transaction pathways [1, 2].

Algebraic reconstruction is important when compromised or inconsistent states are detected. In automata theory, syntactic semigroups encode language-recognition behaviour. In blockchain settings, a transaction history may similarly be regarded as a formal sequence

whose validity depends on accepted transition rules. When a transaction path is perturbed, reconstruction can be interpreted as the process of mapping a corrupted or vulnerable state back into an admissible validation class. This interpretation is supported by work on enveloping semigroups and transformation groups [4].

Finite group theory contributes structural tools for cryptographic modelling. Finite linear groups and nilpotency conditions provide ways of classifying algebraic objects used in computational security [5]. Modular subgroup conditions describe internal stability properties of finite groups [6]. B-algebras generated by modulo integer groups give examples of finite algebraic systems that may be used in discrete-state modelling [7]. Homomorphism counting from Q_8 illustrates how mappings between algebraic structures can be enumerated and interpreted computationally [8]. Such tools are not themselves blockchain protocols, but they support a mathematical language for finite-state security analysis.

Lattice-based cryptography is important because lattice problems are widely regarded as promising bases for post-quantum cryptographic systems. A lattice-based cryptographic scheme for secure blockchain development and financial systems provides direct motivation for introducing a lattice protection coefficient into a blockchain security model [9]. This coefficient does not represent a single implementation detail. Rather, it aggregates the effect of lattice-based authentication, encryption, and post-quantum resistance on the transition of vulnerable transactions into compromised states.

3. Model Variables and Assumptions

Let $S(t)$, $V(t)$, $C(t)$, and $R(t)$ denote secure, vulnerable, compromised, and recovered transaction units at time t, respectively. These variables may represent individual transactions, transaction batches, validator states, or normalized transaction densities. The total active transaction population is

$$N(t) = S(t) + V(t) + C(t) + R(t). \tag{1}$$

The model uses the parameters listed in Table 1. All parameters are assumed to be nonnegative, and Λ and μ are strictly positive.

Table 1: Description of model parameters.

Parameter	Interpretation	Condition
Λ	inflow rate of valid transaction units	$\Lambda > 0$
β	interaction rate between secure and compromised units	$\beta > 0$
γ	progression rate from vulnerable to compromised state	$\gamma > 0$
δ	ordinary validation recovery rate	$\delta \geq 0$
λ	lattice-based cryptographic protection coefficient	$\lambda \geq 0$
σ	semigroup reconstruction efficiency	$\sigma \geq 0$
μ	natural exit or expiration rate of transaction units	$\mu > 0$
ω	return rate from recovered state to secure state	$\omega \geq 0$

The assumptions are:

(A1) New valid transaction units enter the secure class at rate Λ.

(A2) Secure units become vulnerable through interaction with compromised activity at rate βSC.

(A3) Vulnerable units progress to the compromised state at rate γV.

(A4) Lattice-based cryptographic protection prevents vulnerable units from becoming compromised at rate λV.

(A5) Compromised units are restored by ordinary validation at rate δC.

(A6) Compromised units are also restored by semigroup reconstruction at rate σC.

(A7) All active transaction units expire or leave the active system at rate μ.

(A8) Recovered units may re-enter the secure class at rate ωR.

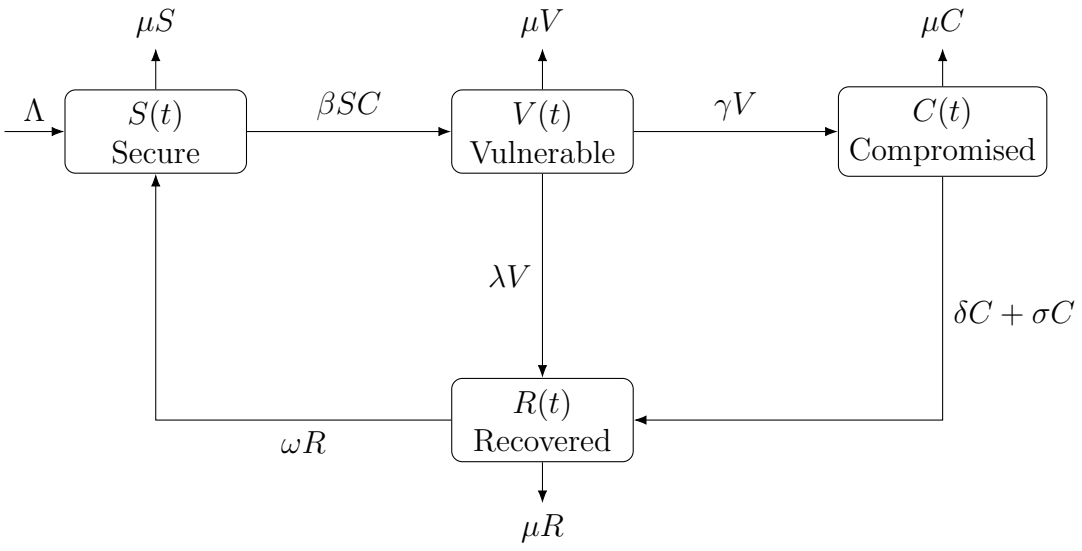

Figure 1: Flow diagram for blockchain transaction security dynamics.

4. Model Formulation

From the assumptions and the flow diagram in Figure 1, the governing system is

$$\frac{dS}{dt} = \Lambda - \beta SC - \mu S + \omega R, \tag{2}$$

$$\frac{dV}{dt} = \beta SC - (\gamma + \lambda + \mu)V, \tag{3}$$

$$\frac{dC}{dt} = \gamma V - (\delta + \sigma + \mu)C, \tag{4}$$

$$\frac{dR}{dt} = \delta C + \lambda V + \sigma C - (\omega + \mu)R. \tag{5}$$

The term βSC captures the interaction of secure transaction units with compromised activity. The parameter λ reduces the vulnerable class and moves protected units into recovery, while σ reduces the compromised class through algebraic reconstruction. The model therefore treats cryptographic prevention and algebraic correction as distinct but complementary mechanisms.

5. Well-Posedness of the Model

5.1. Positivity

Theorem 5.1. *If $S(0) \geq 0$, $V(0) \geq 0$, $C(0) \geq 0$, and $R(0) \geq 0$, then all solutions of (2)–(5) remain nonnegative for $t \geq 0$.*

Proof. On the boundary $S = 0$, equation (2) gives $dS/dt = \Lambda + \omega R \geq 0$. On the boundary $V = 0$, equation (3) gives $dV/dt = \beta SC \geq 0$. On the boundary $C = 0$, equation (4) gives $dC/dt = \gamma V \geq 0$. On the boundary $R = 0$, equation (5) gives $dR/dt = \delta C + \lambda V + \sigma C \geq 0$. Hence the vector field points inward or is tangent on every coordinate boundary of $\mathbb{R}^4_+$. Therefore solutions with nonnegative initial data cannot enter the negative region. □

5.2. Boundedness

Theorem 5.2. *All solutions of (2)–(5) with nonnegative initial conditions are bounded in the region*

$$\Omega = \left\{ (S, V, C, R) \in \mathbb{R}^4_+ : S + V + C + R \leq \frac{\Lambda}{\mu} \right\}. \tag{6}$$

Proof. Adding (2)–(5) gives

$$\frac{dN}{dt} = \Lambda - \mu N. \tag{7}$$

The solution of this scalar equation is

$$N(t) = \frac{\Lambda}{\mu} + \left(N(0) - \frac{\Lambda}{\mu} \right) e^{-\mu t}. \tag{8}$$

Thus $N(t) \leq \max\{N(0), \Lambda/\mu\}$ and $\limsup_{t\to\infty} N(t) \leq \Lambda/\mu$. Hence all trajectories eventually enter and remain in Ω. □

5.3. Existence and uniqueness

Proposition 5.3. *The system (2)–(5) has a unique solution for each nonnegative initial condition.*

Proof. The right-hand side of the model is polynomial in S, V, C, R and is therefore locally Lipschitz continuous on $\mathbb{R}^4_+$. Existence and uniqueness follow from the Picard-Lindelof theorem. Boundedness prevents finite-time blow-up, so the solution exists for all $t \geq 0$. □

6. Equilibrium Analysis

At equilibrium, the right-hand sides of (2)–(5) vanish.

6.1. Attack-free equilibrium

The attack-free equilibrium has $V = C = R = 0$. Equation (2) then gives

$$0 = \Lambda - \mu S, \tag{9}$$

so

$$E_0 = \left(\frac{\Lambda}{\mu}, 0, 0, 0\right). \tag{10}$$

This equilibrium represents a blockchain environment in which transaction activity remains secure and compromised activity is absent.

6.2. Compromised-state equilibrium

Let $E^* = (S^*, V^*, C^*, R^*)$ be an equilibrium with $C^* > 0$. From (4),

$$V^* = \frac{\delta + \sigma + \mu}{\gamma} C^*. \tag{11}$$

Substituting this into (3) gives

$$S^* = \frac{(\gamma + \lambda + \mu)(\delta + \sigma + \mu)}{\beta\gamma}. \tag{12}$$

Equation (5) gives

$$R^* = \frac{\delta C^* + \lambda V^* + \sigma C^*}{\omega + \mu} = \frac{(\delta + \sigma)C^* + \lambda\left(\frac{\delta+\sigma+\mu}{\gamma}\right) C^*}{\omega + \mu}. \tag{13}$$

Finally, equation (2) can be used to determine C^*. A positive compromised-state equilibrium exists if the resulting value of C^* is positive. This occurs when the attack reproduction threshold derived in Section 7 exceeds unity.

7. Blockchain Security Threshold

The attack-related classes are V and C. Let $x = (V, C)^T$. At the attack-free equilibrium, the new attack matrix F and transition matrix W are

$$F = \begin{pmatrix} 0 & \beta\Lambda/\mu \\ 0 & 0 \end{pmatrix}, \qquad W = \begin{pmatrix} \gamma+\lambda+\mu & 0 \\ -\gamma & \delta+\sigma+\mu \end{pmatrix}. \tag{14}$$

The inverse of W is

$$W^{-1} = \frac{1}{(\gamma+\lambda+\mu)(\delta+\sigma+\mu)} \begin{pmatrix} \delta+\sigma+\mu & 0 \\ \gamma & \gamma+\lambda+\mu \end{pmatrix}. \tag{15}$$

Therefore,

$$FW^{-1} = \begin{pmatrix} \dfrac{\beta\Lambda\gamma}{\mu(\gamma+\lambda+\mu)(\delta+\sigma+\mu)} & \dfrac{\beta\Lambda}{\mu(\delta+\sigma+\mu)} \\ 0 & 0 \end{pmatrix}. \tag{16}$$

The blockchain security threshold is the spectral radius of FW^{-1}:

$$\mathcal{R}_s = \frac{\beta\Lambda\gamma}{\mu(\gamma+\lambda+\mu)(\delta+\sigma+\mu)}. \tag{17}$$

The condition $\mathcal{R}_s < 1$ implies that compromised transaction activity declines. The condition $\mathcal{R}_s > 1$ implies that compromised transaction activity can persist.

8. Local Stability of the Attack-Free Equilibrium

The Jacobian matrix of (2)–(5) is

$$J = \begin{pmatrix} -\beta C-\mu & 0 & -\beta S & \omega \\ \beta C & -(\gamma+\lambda+\mu) & \beta S & 0 \\ 0 & \gamma & -(\delta+\sigma+\mu) & 0 \\ 0 & \lambda & \delta+\sigma & -(\omega+\mu) \end{pmatrix}. \tag{18}$$

At E_0, this becomes

$$J(E_0) = \begin{pmatrix} -\mu & 0 & -\beta\Lambda/\mu & \omega \\ 0 & -(\gamma+\lambda+\mu) & \beta\Lambda/\mu & 0 \\ 0 & \gamma & -(\delta+\sigma+\mu) & 0 \\ 0 & \lambda & \delta+\sigma & -(\omega+\mu) \end{pmatrix}. \tag{19}$$

Two eigenvalue contributions are clearly negative through $-\mu$ and $-(\omega+\mu)$ after block reduction. The attack subsystem is governed by

$$A = \begin{pmatrix} -(\gamma+\lambda+\mu) & \beta\Lambda/\mu \\ \gamma & -(\delta+\sigma+\mu) \end{pmatrix}. \tag{20}$$

The trace of A is

$$\operatorname{tr}(A) = -[(\gamma+\lambda+\mu)+(\delta+\sigma+\mu)] < 0. \tag{21}$$

The determinant is

$$\det(A) = (\gamma+\lambda+\mu)(\delta+\sigma+\mu) - \frac{\beta\Lambda\gamma}{\mu}. \tag{22}$$

Using (17),

$$\det(A) = (\gamma+\lambda+\mu)(\delta+\sigma+\mu)(1-\mathcal{R}_s). \tag{23}$$

Therefore $\det(A) > 0$ if and only if $\mathcal{R}_s < 1$.

Theorem 8.1. *The attack-free equilibrium E_0 is locally asymptotically stable if $\mathcal{R}_s < 1$ and unstable if $\mathcal{R}_s > 1$.*

Proof. The non-attack eigenvalue contributions associated with transaction expiration and recovered-state return are negative. The attack subsystem has negative trace for all admissible parameter values. Its determinant is positive exactly when $\mathcal{R}_s < 1$. By the Routh-Hurwitz condition for a second-order system, both eigenvalues of the attack subsystem have negative real parts when $\mathcal{R}_s < 1$. If $\mathcal{R}_s > 1$, the determinant is negative and the attack subsystem has an eigenvalue with positive real part. Thus E_0 is locally asymptotically stable for $\mathcal{R}_s < 1$ and unstable for $\mathcal{R}_s > 1$. □

9. Interpretation of the Threshold

Expression (17) shows how security mechanisms influence long-term blockchain behaviour. The numerator $\beta\Lambda\gamma$ increases attack persistence. A larger transaction inflow Λ increases the number of transaction units exposed to potential attacks. A larger attack interaction coefficient β increases the movement from secure to vulnerable states. A larger progression rate γ increases the movement from vulnerable to compromised states.

The denominator contains the protective and corrective mechanisms. Increasing λ enlarges the factor $(\gamma+\lambda+\mu)$ and thereby reduces $\mathcal{R}_s$. This corresponds to stronger lattice-based cryptographic protection. Increasing σ enlarges the factor $(\delta+\sigma+\mu)$ and thereby reduces $\mathcal{R}_s$. This corresponds to stronger semigroup reconstruction of compromised states. Increasing δ also reduces $\mathcal{R}_s$ through ordinary recovery.

The threshold therefore supports the central thesis of the paper: blockchain security improves when lattice-based cryptographic protection and semigroup reconstruction are increased together. This agrees with algebraic approaches to cryptographic structure, where protection depends not only on encryption strength but also on the ability to

recognise, classify, and reconstruct valid algebraic states [4, 5, 8].

10. Numerical Simulation

Numerical simulations were performed using a fourth-order adaptive Runge-Kutta method. The baseline parameter values used for illustration are shown in Table 2. These values are not intended to represent a particular blockchain implementation. They are selected to demonstrate the qualitative behaviour of the model.

Table 2: Parameter values used for numerical simulation.

Parameter	Baseline value	Enhanced-security value
Λ	50	50
β	0.0008	0.0008
γ	0.20	0.20
δ	0.12	0.12
λ	0.10	0.35
σ	0.08	0.28
μ	0.02	0.02
ω	0.06	0.06

The initial condition used is

$$S(0) = 1200, \qquad V(0) = 80, \qquad C(0) = 40, \qquad R(0) = 0. \tag{24}$$

Under the baseline parameter setting, compromised transactions remain visible for a longer period, while secure transactions recover gradually. The baseline trajectory is shown in Figure 2.

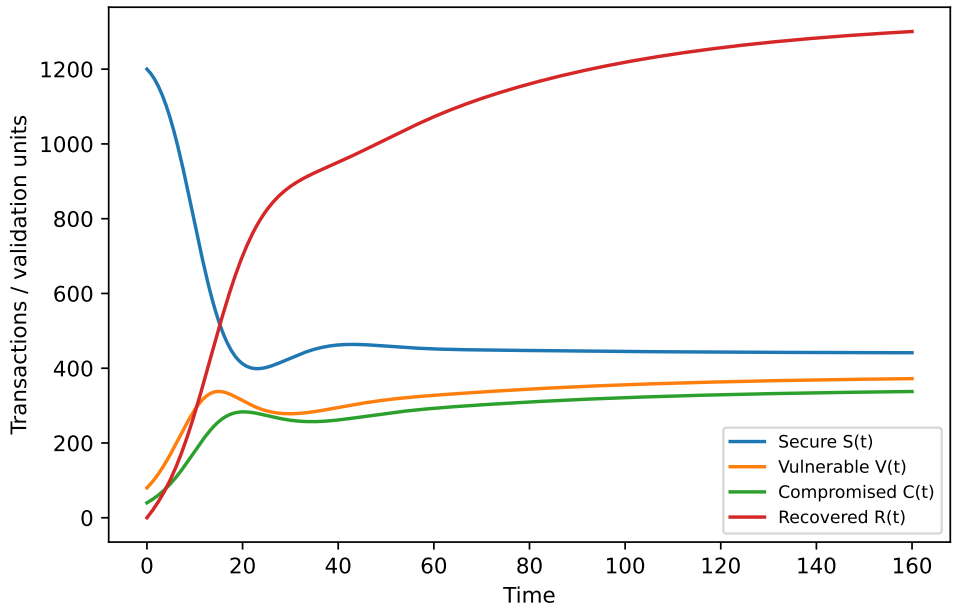

Figure 2: Baseline simulation of secure, vulnerable, compromised, and recovered transaction states.

Under the enhanced-security setting, both λ and σ are increased. This represents stronger lattice-based cryptographic protection and more efficient semigroup reconstruction. Figure 3 shows that vulnerable and compromised transaction levels decline faster than in the baseline case.

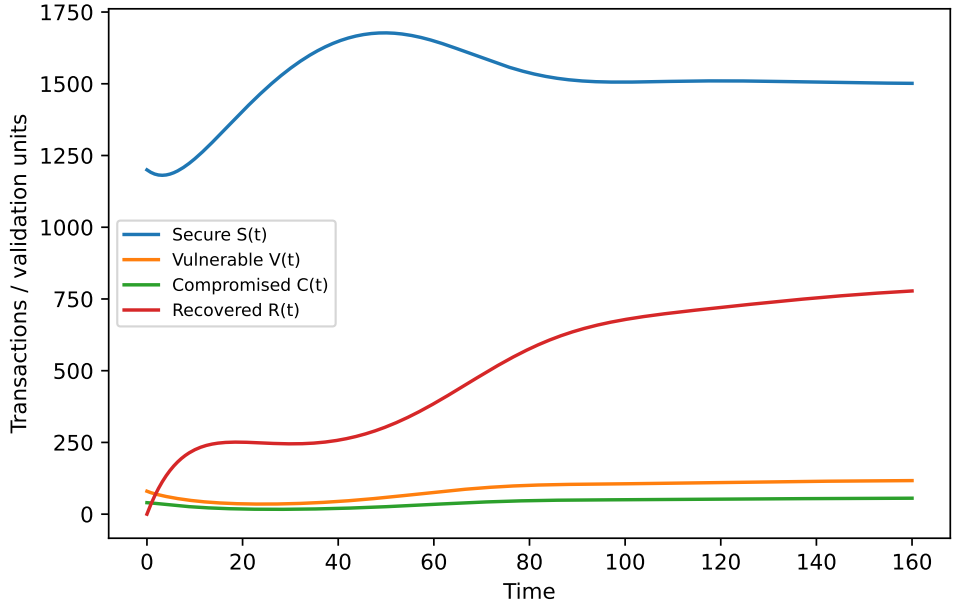

Figure 3: Enhanced-security simulation with larger lattice protection and semigroup reconstruction coefficients.

The threshold surface in Figure 4 illustrates how $\mathcal{R}_s$ changes as λ and σ vary. The

contour $\mathcal{R}_s = 1$ separates the persistence region from the elimination region. Increasing either coefficient moves the system toward the secure region.

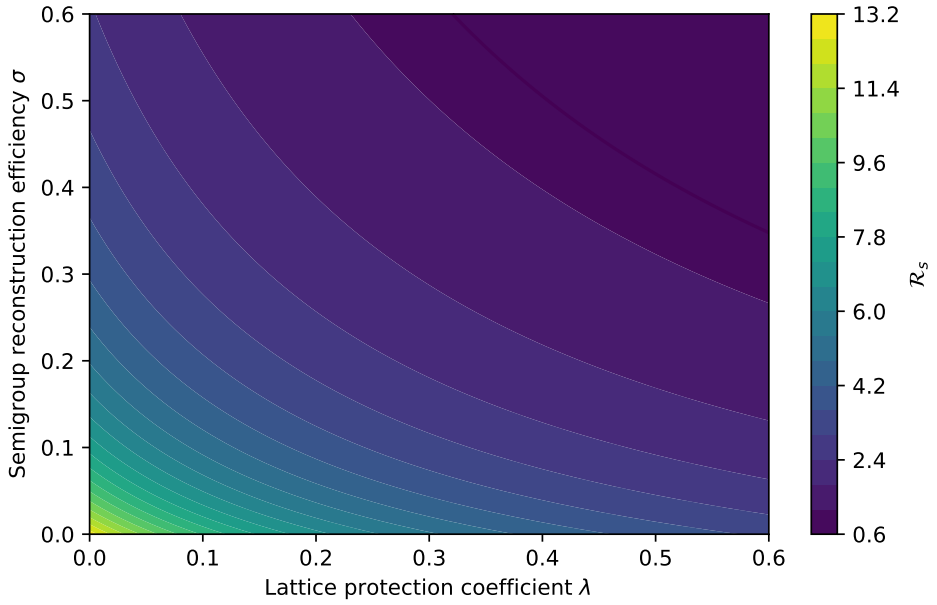

Figure 4: Threshold map showing the effect of lattice protection λ and semigroup reconstruction σ on $\mathcal{R}_s$.

11. Sensitivity Analysis

The normalized forward sensitivity index of $\mathcal{R}_s$ with respect to a parameter p is defined by

$$\Upsilon_p^{\mathcal{R}_s} = \frac{\partial \mathcal{R}_s}{\partial p} \frac{p}{\mathcal{R}_s}. \tag{25}$$

From (17), the indices for selected parameters are:

$$\Upsilon_\beta^{\mathcal{R}_s} = 1, \tag{26}$$

$$\Upsilon_\Lambda^{\mathcal{R}_s} = 1, \tag{27}$$

$$\Upsilon_\gamma^{\mathcal{R}_s} = 1 - \frac{\gamma}{\gamma + \lambda + \mu}, \tag{28}$$

$$\Upsilon_\lambda^{\mathcal{R}_s} = -\frac{\lambda}{\gamma + \lambda + \mu}, \tag{29}$$

$$\Upsilon_\delta^{\mathcal{R}_s} = -\frac{\delta}{\delta + \sigma + \mu}, \tag{30}$$

$$\Upsilon_\sigma^{\mathcal{R}_s} = -\frac{\sigma}{\delta + \sigma + \mu}, \tag{31}$$

$$\Upsilon_\mu^{\mathcal{R}_s} = -1 - \frac{\mu}{\gamma + \lambda + \mu} - \frac{\mu}{\delta + \sigma + \mu}. \tag{32}$$

The positive indices show parameters that increase attack persistence. The negative indices show parameters that reduce attack persistence. Figure 5 presents the numerical sensitivity indices for the baseline parameter values.

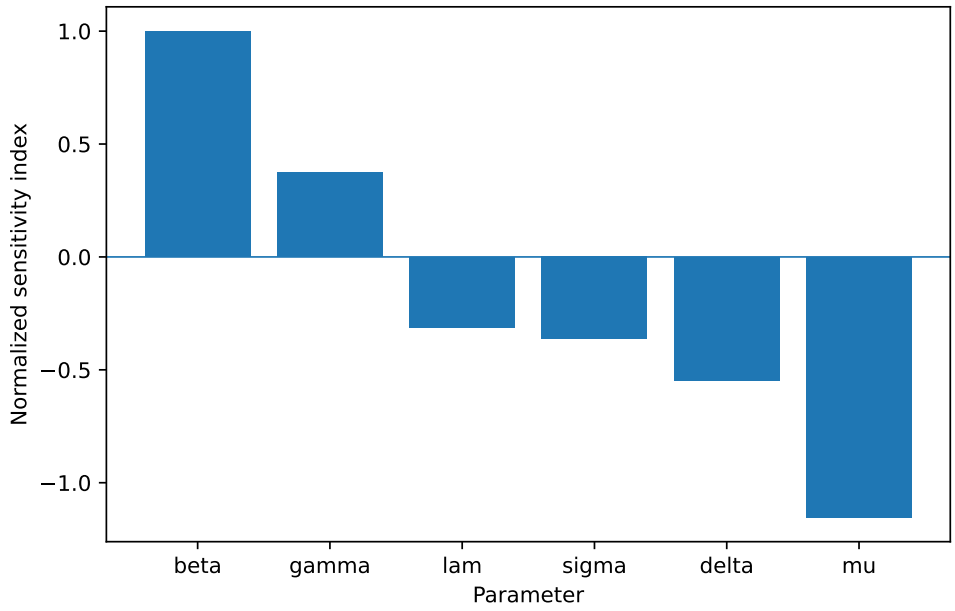

Figure 5: Normalized sensitivity indices for selected parameters.

The sensitivity results confirm that attack interaction β has a strong positive effect on $\mathcal{R}_s$. In contrast, lattice protection λ, ordinary recovery δ, semigroup reconstruction σ, and transaction expiration μ reduce $\mathcal{R}_s$. This means that blockchain security improves when the system reduces attack contact, strengthens cryptographic protection, accelerates validation recovery, and improves algebraic reconstruction.

12. Discussion

The model provides a mathematical explanation of how algebraic and cryptographic tools can influence blockchain security dynamics. The lattice coefficient λ represents post-quantum protection against vulnerability progression. Its effect is most visible in the threshold denominator, where increasing λ reduces the chance that vulnerable transaction units contribute to persistent compromised activity. This agrees with the role of lattice-based cryptographic schemes in secure blockchain development and financial systems [9].

The semigroup coefficient σ represents algebraic reconstruction. Its interpretation is supported by the use of semigroup and automaton frameworks in syntactic reconstruction and transformation systems [1, 2, 4]. In a practical blockchain environment, such reconstruction could correspond to rule-based restoration, symbolic validation, consensus-level correction, rollback of invalid state transitions, or reclassification of transaction pathways.

The model also connects to finite algebraic structures. Group classification, modular subgroup theory, B-algebras, and homomorphism counting provide examples of how finite algebraic properties can inform the design of structured security systems [5, 6, 7, 8]. Although the model is deterministic, it can be extended to stochastic transaction networks, graph-based blockchain topologies, or agent-based validator simulations.

The financial motivation is also important. Secure digital transactions affect confidence in digital finance, especially in environments undergoing policy changes in currency systems or digital payment structures [12]. A mathematical security model can therefore contribute to both technical blockchain design and broader financial-system resilience.

13. Conclusion

This paper developed a hybrid deterministic mathematical model for blockchain transaction security incorporating lattice-based cryptographic protection and algebraic semigroup reconstruction. The blockchain transaction environment was divided into secure, vulnerable, compromised, and recovered states. The model was shown to be positive, bounded, and well posed. A blockchain security threshold $\mathcal{R}_s$ was derived, and the attack-free equilibrium was shown to be locally asymptotically stable when $\mathcal{R}_s < 1$.

The analysis shows that attack persistence increases with the attack interaction rate and the vulnerability progression rate. It decreases with stronger lattice-based protection, faster recovery, and more efficient semigroup reconstruction. Numerical simulations confirmed that combined improvement in λ and σ produces a more resilient blockchain environment. Future work may extend the model to stochastic networks, graph-based validation structures, delay differential equations, fractional-order models, and empirical calibration using real blockchain transaction data.

Acknowledgement

The author acknowledges the Department of Mathematics, Akwa Ibom State University, Nigeria, for providing an academic environment that supports research in mathematical modelling, algebra, and computational mathematics.

Funding

The author received no specific funding for this work.

Conflict of Interest

The author declares no conflict of interest.

Copyright and License

References

[1] M. N. John, O. I. Stephen, R. Akerejola, and C. J. Alhassan, "Differential semigroups of automaton perturbations and incremental syntactic reconstruction," 2026.

[2] M. N. John, O. I. Stephen, R. Akerejola, and C. J. Alhassan, "A categorical framework for syntactic semigroups and language transformations," *International Journal of Applied Mathematics*, vol. 39, no. 1s, 2026.

[3] I. U. Udo-Akpan and M. N. John, "Enhanced algorithm for modular isomorphism problem resolution in small group orders," 2024.

[4] M. John, "Algebraic and topological analysis of enveloping semigroups in transformation groups: proximal equivalence and homomorphic image," *IPHO-Journal of Advance Research in Mathematics and Statistics*, vol. 2, no. 12, pp. 21–27, 2024.

[5] M. N. John, "On the structure and classification of finite linear groups: a focus on Hall classes and nilpotency," 2023.

[6] M. N. John, "Modularity in finite groups: characterizing groups with modular σ-subnormal subgroups," 2023.

[7] M. N. John and E. E. Bassey, "On finding B-algebras generated by modulo integer groups $\mathbb{Z}_n$," 2023.

[8] M. N. John, E. E. Bassey, O. G. Udoaka, O. J. Tom, and P. O. Asukwo, "On finding the number of homomorphism from Q_8," 2023.

[9] F. A. Effiong, E. H. Enyiduru, L. E. Effiong, M. I. Sampson, "Lattice-based cryptographic scheme for secure blockchain development and financial systems," *Journal of Science Education and Humanities*, vol. 7, no. 1, 2023.

[10] M. N. John, "Teaching abstract algebra: group and subgroup concepts in colleges of education in Nigeria beyond COVID-19," 2022.

[11] P. N. Michael John, "Computational analysis of a nonlinear heat transfer equation," 2018. doi: 10.13140/RG.2.2.15117.28641.

[12] U. Etim and M. John, "Regional analysis of the currency redesign policy on Nigeria's socioeconomic, business and financial landscape," 2024.

[13] O. J. Tom, E. John, U. M. Udo, and M. N. John, "Ulm function analysis of full transitivity in primary abelian groups," 2024.

[14] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008.

[15] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed. Boca Raton, FL: CRC Press, 2020.

[17] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*. New York: Springer, 2008.

[18] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.

[19] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Indianapolis: Wiley, 2008.

[20] S. H. Strogatz, *Nonlinear Dynamics and Chaos*, 2nd ed. Boulder, CO: Westview Press, 2015.