

Designing resilient infrastructure for smart cities using blockchain and cryptography

Lowlesh Nandkishor Yadav [†]

*Department of Computer Engineering
Suryodaya College of Engineering & Technology
Nagpur 440034
Maharashtra
India*

Tanya Singh ^{*}

*School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India*

Anupama Abhijeet Deshpande [§]

*Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India*

K. Shree Jayaram [‡]

*MAHER Innovation & Incubation Centre
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India*

[†] E-mail: lowlesh.yadav@gmail.com

^{*} E-mail: dean.academics@niu.edu.in (Corresponding Author)

[§] E-mail: anupama.deshpande1@vit.edu

[‡] E-mail: sjayaram@gmail.com

Naveen Jain^{*}

Department of Mechanical Engineering
Shri Shankaracharya Institute of Professional Management & Technology
Raipur 492015
Chhattisgarh
India

Abstract

The smart city development has been grown faster way, so that such smart cities need requirement that it should be safe, reliable as an infrastructure that can handled the complex system for computations of data in the real time environment. Cryptographic methods make data even safer, more private, and more reliable. The study discuss the blockchain and cryptographic models that used for building smart city which more reliable and resilient to attacks. The proposed approach maintains the stability, efficiency, and longevity of urban systems by emphasizing consensus models, security frameworks, and resiliency indicators.

Subject Classification: 11T71, 94A60.

Keywords: Blockchain, Cryptography, Smart cities, Resilience, Security.

I. Introduction

The use of modern tools to improve life, which has revolutionized how people live in smart cities. As more people migrate into cities, it becomes difficult for them to keep their buildings, data management, and service delivery safe and effective [1]. Linked systems and real-time data processing are two crucial things that smart cities need. This means that the infrastructure must be strong, safe, and able to manage a lot of different problems and threats [2, 3, 4]. Blockchain is a great way to keep smart city systems safe because it is open, decentralized, and can't be changed. Cryptography does more to protect data by making sure it is safe and correct. This article looks at how blockchain and security can be used to build reliable infrastructure for smart cities [5]. The idea is to make sure that it's safe to share information, make decisions, and get in touch with people.

As shown in Figure 1, we offer a new way to fix issues with smart city plans by focusing on robustness metrics, cryptographic security frameworks, and consensus models. The suggested ways are meant to offer long-lasting safety and security, letting cities use safe, effective, and environmentally friendly tech solutions to run their cities [6, 7].

II. Mathematical Methodology

A. Blockchain Consensus Model

With the use of blockchain technology in this, the blockchain uses the fundamental model as PoS and PoW for the validation of transaction where each node has approve it [8, 9, 10].

^{*} E-mail: n.jain@ssipmt.com

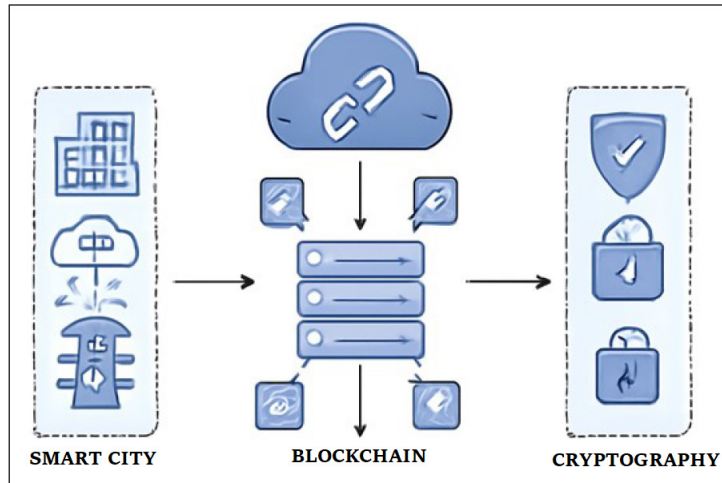


Figure 1
Resilient Infrastructure for Smart Cities: Blockchain and Cryptography Integration

Transaction Throughput (TPS):

$$TPS = \frac{\text{Total Transactions}}{\text{Total Time}}$$

Latency (ms):

$$\text{Latency} = \frac{\text{Time to Confirm a Transaction}}{\text{Total Number of Transactions}} \quad (1)$$

Security Level:

$$S = f(\text{Hash Rate}, \text{Attack Resistance}, \text{Fault Tolerance})$$

Energy Consumption:

$$E = \text{Energy per Transaction} * \text{Number of Transactions}$$

Proof of Work (PoW):

$$PoW = \text{Hash Difficulty} * \text{Computation Time}$$

Proof of Stake (PoS):

$$PoS = \text{Stake Weight} * \text{Validator Selection Probability}$$

Practical Byzantine Fault Tolerance (PBFT):

$$PBFT = \frac{(3n + 1)}{2 \text{ Nodes (for fault tolerance)}} \quad (2)$$

Delegated Proof of Stake (DPoS):

$$DPoS = \frac{n \text{ Delegates}}{k \text{ Votes}} \quad (3)$$

Consensus Efficiency:

$$\text{Efficiency} = \frac{\text{Transaction Throughput}}{\text{Energy Consumption}} \quad (4)$$

B. Cryptographic Security Model

The cryptographic security model uses encryption methods, like hashing and asymmetric key cryptography, to keep data safe, make sure contact is safe, and stop people from getting in without permission [11, 12].

Encryption Algorithm Efficiency:

$$\text{Encryption Speed} = \frac{\text{Data Size}}{\text{Time}} \quad (5)$$

Key Length and Security:

$$\text{Security} = f(\text{Key Length}) \quad (6)$$

Hashing Function Performance:

$$\text{Hashing Speed} = \frac{\text{Number of Hashes}}{\text{Time}} \quad (7)$$

Symmetric Key Encryption:

$$C = E_{k(P)} \quad (8)$$

Asymmetric Key Encryption:

$$C = E_{k_{pub}(P)} \quad (9)$$

Digital Signature:

$$\text{Signature} = \text{Sign}_{k(P)} \quad (10)$$

Key Exchange (Diffie-Hellman):

$$K = g^{ab} \bmod p \quad (11)$$

RSA Security:

$$C = P^e \bmod n \quad (12)$$

Elliptic Curve Cryptography (ECC):

$$C = P * k \quad (13)$$

AES (Advanced Encryption Standard):

$$C = \text{AES}(P, K) \quad (14)$$

C. Resilience and Reliability Metrics

The reliability analysis done by the reliability check, the mathematical formula for this given below [13]:

System Reliability:

$$R = \frac{\text{Successful Operations}}{\text{Total Operations}} \quad (15)$$

Fault Tolerance:

$$FT = \frac{\text{Failures Tolerated}}{\text{Total Failures}} \quad (16)$$

Recovery Time:

$$RT = \frac{\text{System Downtime}}{\text{Failure Events}} \quad (17)$$

Mean Time to Failure (MTTF):

$$MTTF = \frac{1}{\lambda} \text{ (Where } \lambda \text{ is the failure rate)} \quad (18)$$

Mean Time to Repair (MTTR):

$$MTTR = \frac{\text{Total Repair Time}}{\text{Number of Repairs}} \quad (19)$$

Availability:

$$A = \frac{\text{Uptime}}{(\text{Uptime} + \text{Downtime})} \quad (20)$$

Service Level Agreement (SLA):

$$SLA = \frac{\text{Actual Service Time}}{\text{Expected Service Time}} \quad (21)$$

Data Integrity:

III. Cryptographic Algorithm

A cryptographic method is picked based on how safe it is, how fast it can be used, and how well it can be expanded. Algorithms like AES for encryption and RSA for key sharing make sure that both security and speed are high.

Key Size (n):

$$n = \text{Length of the key (in bits)}$$

Ciphertext (C):

$$C = E_{k(P)} \quad (22)$$

(Where C is the ciphertext, E_k is the encryption function, and P is the plaintext)

Encryption Speed (S):

$$S = \frac{\text{Data Size}}{\text{Time Taken}} \quad (23)$$

$$O = \frac{(\text{Total Computation Time})}{(\text{Total Encryption Time})} \quad (24)$$

Security Level (L):

$L = f(\text{Key Length, Hash Function Strength, Resistance to Attacks})$

Key Exchange (Diffie-Hellman):

$$K = g^{ab} \bmod p \quad (25)$$

Hash Function Collision Resistance:

$$P(\text{Collision}) = \frac{(\text{Number of Collisions})}{(\text{Total Hashes})} \quad (26)$$

Symmetric Encryption (AES):

$$C = AES(P, K) \quad (27)$$

Asymmetric Encryption (RSA):

$$C = P^e \bmod n \quad (28)$$

Digital Signature:

$$Signature = Sign_{k(P)}$$

(29)

Elliptic Curve Encryption:

$$C = P * k$$

(30)

IV. Results and Analysis

Based on key success measures, Table 1 shows a review of different blockchain consensus models. Proof of Work (PoW) has the slowest transaction rate (25 TPS) and the longest delay (2000 ms).

Table 1
Blockchain Consensus Model Performance Metrics

Consensus Model	Transaction Throughput (TPS)	Latency (ms)	Security Level (1-10)	Energy Consumption (J)
(PoW)	25	2000	9	100
(PoS)	100	500	8	30
(PBFT)	500	150	10	50
(DPoS)	150	400	8	20

It also uses a lot of energy (100 J), but it has the best level of security (9).

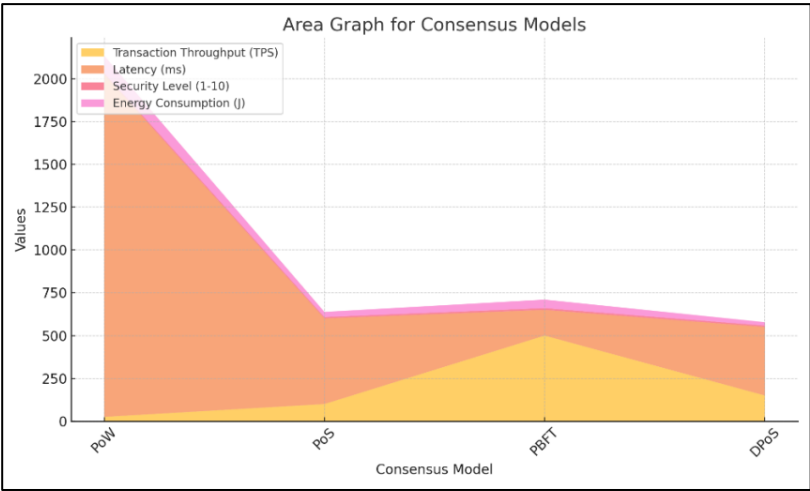


Figure 2
Consensus Model Performance Breakdown

Proof of Stake (PoS) has a slightly lower level of security but better speed (100 TPS) and lower latency (500 ms). It also uses less energy (30 J) (in Figure 2).

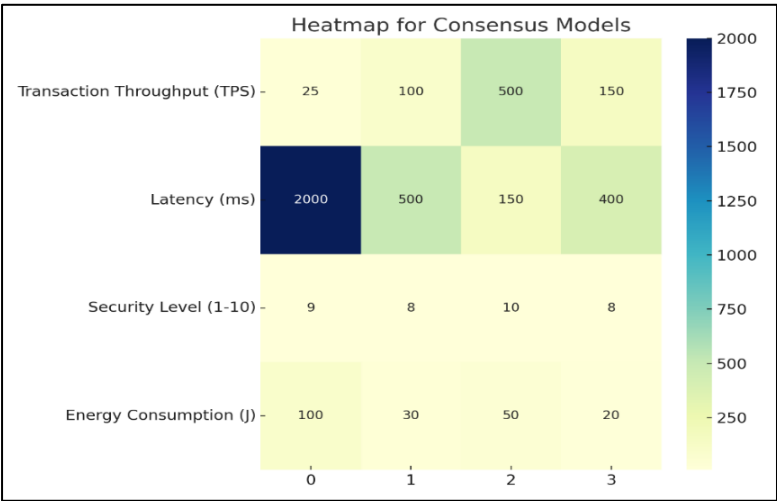


Figure 3
Consensus Model Comparison Heatmap

Although it uses 50 J of energy, Practical Byzantine Fault Tolerance (PBFT) has the best speed (500 TPS) and security (10) (shows in Figure 3). Delegated Proof of Stake (DPoS) has 150 TPS, 400 ms delay, 8 security levels, and uses the least amount of energy (20 J).

V. Conclusion

When you combine blockchain and security models, you get a strong way to build infrastructure that will last in smart cities. Cities can protect communication, data accuracy, and privacy by using cryptography's data security systems and blockchain's decentralised decision mechanisms. In addition, resilience and dependability measures let you check how well a system can handle outages. This method not only makes smart city systems safer and more efficient, but it also encourages long-term, future-proof urban growth, making places safer and more stable for people to live.

References

[1] K. Achuthan, S. Sankaran, S. Roy, and R. Raman, "Integrating sustainability into cybersecurity: Insights from machine learning based topic modeling," *Discov. Sustain.*, vol. 6, p. 44 (2025).

[2] S. Anjum, A. Ahmed, R. Kurup, S. Kidiya, and S. Kureshi, "Blockchain based image steganography," *Int. J. Adv. Comput. Theory Eng.*, vol. 14, no. 1, pp. 147–152 (May 2025).

- [3] F. Z. Chentouf and S. Bouchkaren, "Security and privacy in smart city: A secure e-voting system based on blockchain," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 13, pp. 1848–1857 (2023).
- [4] R. Joysoyal, S. S. Uddin, T. Islam, S. K. Sarker, L. Li, F. Ahsan, U. A. Bhatti, and E. I. Zafir, "Blockchain for sustainable city transformation: A review on Bangladesh," *Eng. Rep.*, vol. 6, p. e12948 (2024).
- [5] Z. A. Kaiser, "Smart governance for smart cities and nations," *J. Econ. Technol.*, vol. 2, pp. 216–234 (2024).
- [6] A. Pliatsios, K. Kotis, and C. Goumopoulos, "A systematic review on semantic interoperability in the IoE-enabled smart cities," *Internet Things*, vol. 22, p. 100754 (2023).
- [7] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, "Sustainable smart cities: Convergence of artificial intelligence and blockchain," *Sustainability*, vol. 13, p. 13076 (2021).
- [8] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain, and P. Khobragade, "Blockchain technology in pharmaceutical supply chain: Ensuring transparency, traceability, and security," *J. Stat. Manage. Syst.*, vol. 27, no. 2, pp. 417–428 (2024), doi: 10.47974/JSMS-1266.
- [9] N. Tura and V. Ojanen, "Sustainability-oriented innovations in smart cities: A systematic review and emerging themes," *Cities*, vol. 126, p. 103716 (2022), doi : 10.47974/JDMSC-1921.
- [10] D. Goyal, A. Kumar, Y. Gandhi, and V. Khetani, "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 703–714 (2024).
- [11] S. Yadav, R. Sharma, A. Dabas, C. Arora, G. Mitra, A. Aggarwal, A. Rehalia, S. Sanyal, and M. Arora, "Improved security in credit cards via duplicitous contract detection," *J. Inf. Optim. Sci.*, vol. 46, no. 1, pp. 75–79 (2025), doi: 10.47974/JIOS-1853.
- [12] M. Yi, D. Chen, T. Wu, M. Tao, M. S. Sheng, and Y. Zhang, "Intelligence and carbon emissions: The impact of smart infrastructure on carbon emission intensity in cities of China," *Sustain. Cities Soc.*, vol. 112, p. 105602 (2024).
- [13] F. Zeng, C. Pang, and H. Tang, "Sensors on Internet of Things systems for the sustainable development of smart cities: A systematic literature review," *Sensors*, vol. 24, p. 2074 (2024).