Journal of Computer Science

Research Article

Blockchain-NFV for Smart Digital and Secure Physical Structures in E-Government, Healthcare, and Network Systems

Hayder Abdulsattar Nahi[1], Akmam Majed Mosa[1], Ebtehal Akeel Hamed[2] and Rusul A. Salman[3]

[1]*Computer Center, Al Qasim Green University, Babylon 51013, Iraq*
[2]*College of Physical Education and Sports Sciences, Al Qasim Green University, Babylon 51013, Iraq*
[3]*College of Veterinary Medicine, Al Qasim Green University, Babylon 51013, Iraq*

Article history
Received: 27-06-2025
Revised: 05-12-2025
Accepted: 12-02-2026

Corresponding Author:
Hayder Abdulsattar Nahi
Computer Center, Al Qasim Green University, Babylon 51013, Iraq
Email: haider.satar@uoqasim.edu.iq

Abstract: This paper proposed a combined model that melds Blockchain technology with Network Function Virtualization (NFV) to promote many areas, such as smart, secure, and scalable physical and digital infrastructures in E-Government, Healthcare, and Network Systems. The model treats the principal objections in conventional systems, including centralization, slowed service deployment, and restricted safety. By employing decentralized Digital Identity Decentralized identifiers (DIDs), smart contracts, and Virtual Network Functions (VNFs), the system guarantees boosted trust, auditability, and elasticity. The quantitative outcomes observed in the experiments showed a highly significant improvement. The review demonstrated a 46% reduction in access time, while the transaction throughput rate increased by more than 140%, exceeding previous efforts, and an 80% reduction in deployment time for service. Applying the model in the health care domain shows an overall session duration drop from 22 minutes to 6 minutes, resulting in an improvement of 73% overall. The reliability metrics assessment for the overall review resulted in a reliable classification of 5 out of 5 for the overall assessment based on our results, data integrity, conformance to terms of service, and resistance to attacks. Given all of the above, the presented model is identified as a promising environment for future digital transformation in terms of assuring security, capacity, and adaptability for critical issues.

Keywords: Blockchain, E-Government, Healthcare, Steganalysis, Virtualization

Introduction

The dramatic expansion in the provision of services to individuals has been driven by the digital transformation in many sectors such as healthcare and telecommunications (Adnan et al., 2022; Ahmad and David, 2024; Alam et al., 2020). Data integrity and secure communications are among the most important aspects of these services, making them a target for cybercriminals and cyber threats (Alexopoulos et al., 2019). Conventional centralized infrastructure samples are frequently insufficient to address the dynamic and distributed nature of these scopes. There are many papers that address some challenges through a suggested hybrid architecture that combines the decentralization and trust of Blockchain with the flexibility and scalability of Network Function Virtualization (NFV) (Alrowaily et al., 2023; Barbieri et al., 2023).

Blockchain technology encloses secure exchange of data, transparent auditing, and protected records (Alexopoulos et al., 2019; Bodkhe et al., 2020). In the meantime, NFV gives the ability to the network functions considered virtualized and dynamically managed to rely on real-time service requests. In conjunction, these technologies handle the miscellaneous demands of present-day digital infrastructures by supplying end-to-end security, adaptability, and intelligence.

As e-government frameworks continue to develop, warranting the security and thoroughness of their underlying physical infrastructure has become an

essential (Douha et al., 2022). The combination of prominent technologies, including Blockchain, Network Function Virtualization (NFV), and Quantum Key Distribution (QKD), provides favorable solutions to promote the security, scalability, and flexibility of these systems (Durga et al., 2022). Blockchain supplies a decentralized and protected field for data integrity and confidence, while NFC provides resilient and economic running of network services (Egala et al., 2021). QKD shows a quantum-level layer of encryption, enabling the secure distribution of cryptographic keys that depend on the rules of quantum mechanics, just like that, making interception virtually not possible (Elisa et al., 2023). These technologies have the ability to improve physical security by providing real-time monitoring, automatic detection of threats, and quantum-proof data processing. As healthcare advances with digital transformation, the volume of patient information processed has grown exponentially in recent times (Haleem et al., 2021). Blockchain technology and Network Function Virtualization (NFV) are two of the more current solutions that are being used to improve healthcare IT systems (Alam et al., 2020). Blockchain technology provides a secure, decentralised, and tamper-proof ledger of all transactions that create an environment of trust, data integrity, and traceability in all healthcare connected entities. In addition, NFV provides the capability to dynamically provision and manage virtualized healthcare services that allow users to move away from traditional models of delivery. Blockchain technology and network function virtualization provide a secure method for sharing data and coordinate services in real time so that healthcare systems can respond rapidly to fluctuations in demand, consequently increasing the security, efficiency, and resiliency of healthcare operations (Hussain et al., 2024).

This paper investigates the symbiotic possibilities of stimulus to a Hybrid Blockchain-NFV combination in building smart digital and secure physical structures over critical fields like e-government, healthcare, and broader network systems. Through investigating their collaborative ability to improve data integrity, service agility, and infrastructure resilience, the paper looks into how these technologies have the ability to handle existing security and performance difficulties.

Literature Review

The combination of blockchain technology with NFV has emerged as a transformative process to boost security, scalability, and elasticity in smart digital and physical organizational structures and facilities. This gathering leverages the decentralized, immutable nature of blockchain and the dynamic, software-based abilities of NFV to handle developing challenges in critical parts such as e-government, healthcare, and network systems. In the table below, a summary of previous studies is presented that are very similar to the proposed system.

Proposed System

The proposed hybrid framework is structured into five layers, the Application Layer, Service Domain, Blockchain Layer, NFV Layer, and Infrastructure Layer (Fig. 1).

Table 1: Summary of Previous Works on Blockchain–NFV Combination

Application Area	Key Paper Contribution	Main Advantages and Results	References
E-Government Systems	Using Blockchain–NFV hybrid models to secure national data management, legal records, and transactional information.	Increases transparency, prevents tampering, decreases fraud, and enables automated policy enforcement via smart contracts.	(Jawdhari and Abdullah, 2022; Koo, 2019, Koroye, 2023; Li et al., 2024; Liu et al., 2020)
Healthcare Systems	Integration of Blockchain and NFV for secure, interoperable medical data exchange between hospitals, laboratories, insurers, and governmental entities.	Guarantees for privacy, data integrity, traceability of patient records, and efficient management of EHR analytics and monitoring functions.	(Ahmad and David, 2024; Maurya et al., 2025; Nahi et al., 2025a-b; Nalini and Mageshwari, 2017)
Telecommunication Networks (IoT, 5G, Edge)	Deployment of Hybrid Blockchain–NFV architecture for decentralized network service control and automation.	Improves service scalability, enables decentralized trust via consensus, and eliminates single points of failure.	(Patil et al., 2021; Pattaranantakul et al., 2018; Rahman et al., 2024a-b; Santos, 2025)
Smart Physical Infrastructure (Smart Cities, ITS, Industry 4.0)	Application of Blockchain–NFV to secure interactions among sensors, actuators, and autonomous devices.	supplies trusted data exchange, real-time control, and auditable transactions for intelligent environments.	(Nalini and Mageshwari, 2017; Shahraki et al., 2021; Varma and Kumar, 2023; Zhu and Cao, 2021)

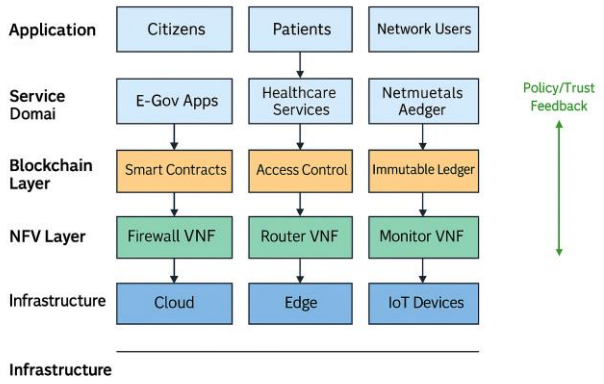

Fig. 1: proposed system

Each layer plays a specific role while maintaining interconnectivity and complementarity with other layers.

Application Layer

This topmost layer interfaces directly with end-users such as citizens, patients, administrators, and devices. It enables the initiation of service requests through web or mobile platforms (1). These requests are relayed to the Service Domain for further processing.

Algorithm 1: Processing User Requests

```
Input request(user_id, service_type)
Output Validated Service Call
procedure HandleUserRequest(request)
 Extract user_id, service_type from request
Forward to ServiceDomain
end procedure
```

Service Domain Layer

Through the Service Layer, users can input information to create workflows that will be executed. Within the Service Layer is a collection of applications that utilize the user inputs in order to create workflows based on the algorithms created by the application's Algorithm (2). Additionally, the Service Layer provides access to e-government, healthcare, and network management applications, as well as the functionality to validate a user's identity and access to applications using Smart Contracts when accessing the Blockchain Layer via the Service Layer. Furthermore, the Service Layer provides access to Network Function Virtualization Services to allow dynamic resource provisioning.

Algorithm 2: Implementing a Service Domain Workflow

```
Input request(user_id, service_type)
Output Validated Service Call
 procedure ServiceDomain(request)
 Validate service_type
 result ← CheckBlockchain(user_id)
 if result = Verified then
 vnf_config ← GenerateVNFRequest(service_type)
 TriggerNFVOrchestration(vnf_config)
else
Reject request
 end if
end procedure
```

Blockchain Layer

This portion of the architecture essentially serves as the "trust anchor" of the entire architecture by automating the service logic via smart contracts and verifying the user's ID via Decentralized Identity Management (DID) while maintaining an immutable log of all transactions (Algorithm 3). In addition, the analytic data collected from the Monitoring NFV Functions' data is utilized by the Blockchain for both adaptive trust evaluations and ongoing Policy Enforcement.

Algorithm 3: Blockchain Verification.

```
1.  Input request(user_id, service_type)
2.  Output Validated Service Call
3.  procedure CheckBlockchain(user_id)
4.  Fetch DID record from blockchain
5.   If DID is valid and active, then
6.  return Verified
7.  else
8.  return Rejected
9.  end if
10. end procedure
```

NFV Layer

The NFV layer manages the orchestration of virtual network functions (VNFs) such as firewalls, routers, load balancers, and monitoring tools. The VNF is instantiated dynamically in response to a service requirement from the Service Domain and validated by Blockchain. This layer also monitors service behavior and returns logs to the Blockchain Layer Algorithm (4).

Algorithm 4: NFV Orchestration.

```
1.   1 Input request(user_id, service_type)
2.  Output Validated Service Call
3.  Procedure TriggerNFVOrchestration(vnf_config)
4.   for each vnf in vnf_config do
5.  Deploy the VNF to a suitable node
6.  Configure monitoring and logging
7.  end for
8.  SendLogToBlockchain(vnf_deployment)
9.  end procedure
10.
```

Infrastructure Layer

At the base of the framework, the Infrastructure Layer includes cloud servers, edge devices, and IoT endpoints. It provides the computing and storage environment where VNFs and service workloads are executed. This layer adheres to policies authenticated by the Blockchain Layer

and is dynamically managed by the NFV orchestrator Algorithm (5).

Algorithm 5: Infrastructure Deployment and Implementation

1. Input request (user_id, service_type)
2. Output Validated Service Call
3. procedure Deploy And Execute (vnf, node)
4. Allocate resources on the node
5. Launch container/VM for VNF
6. Start service and monitor SLA compliance
7. end procedure

Materials and Architecture

This study focuses on a hybrid architecture that combines blockchain and Network Functions Virtualization (NFV) technologies to improve security, scalability, and operational flexibility in digital systems (e.g., e-government, healthcare, and telecommunications networks). This section provides a succinct description of the data used, the architecture, the implementation environment, and the evaluation methods.

Data and Sources

We used simulated data with 1,000 service requests across two types of scenarios:

- E-government identity verification scenario.
- Healthcare environment medical data exchange scenario.
- Each request contains:

- User ID
- Service type
- Access policies
- Security requirements

Also generated data similar to IoT device data (e.g., Latency, Packet Rate, VNF Load) to simulate a true-to-life condition.

Architecture Model

The proposed architecture consists of five interconnected layers that are presented above in the proposed system.

The digital infrastructure for e-government, healthcare, and network systems provided by this model proposes a combination of NFV components with blockchain functionality to create a natively secure, scalable, and programmable digital infrastructure (Fig. 2).

The figure depicts a layered model that integrates blockchain functions (distributed ledger, smart contracts, identity verification) with NFV functions (firewall, routing, monitoring) to enable flexible, secure, and scalable services in e-government, healthcare, and network systems.

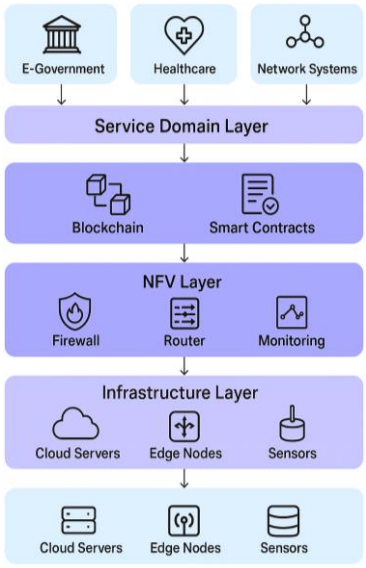

Fig. 2: Hybrid Blockchain–NFV for Safe Architectural along with Intelligent Digital Infrastructure

The diagram depicts the request path from the application layer to the service layer, blockchain verification, then the on-demand deployment of virtual network functions, followed by execution in the cloud, endpoint nodes, and sensors.

The Method of Work

In this study, we have created and assessed a combined solution that uses the security and trustworthiness of Blockchain and the flexibility and scaling potential of NFV. The research methodology includes four key areas: Architecture Design, Data Modeling, Simulation Environment Setup, and Indicators for Evaluation.

Design of Architecture

The architecture of the proposed Solution is layered according to a typical Telecom Network Reference Model. The components are listed below:

- Application Layer
- Service Layer
- Blockchain Layer
- NFV Layer
- Infrastructure Layer

Smart contracts are employed as the mechanism for automating identity verification procedures and access control in addition to enforcing policy. The technologies used for NFV enable the VNF deployment in a dynamic and virtualized manner, e.g., Firewalls, Routing, and Monitoring.

Modeling of Data

For the purposes of this paper, simulated 1,000 service requests under 2 scenarios:

1. E-Government Identity Verification Scenario
2. Medical Data Exchange Scenario in a Healthcare System

Every service request was made up of 4 elements:

1) Service type
2) User Characteristics
3) Security Requirements
4) Access Policy

The second group of simulated data was designed to reflect the real-time operation of an Internet of Things (IoT) System via Artificial Latency, Packet Rate, and VNF Load.

Implementation Environment

The experiments were performed using:

- Python version 3.11
- Mininet-VNF platform
- Operating System of Ubuntu 22.04
- Intel Xeon processor and 32GB RAM
- Five blockchain nodes to perform verification
- Deployment of 20 Virtual Network Functions (VNFs)

Evaluation Procedures

The system was assessed using these metrics:

- Latency
- Throughput
- Service deployment time
- Auth verification time
- Trust score

There were 10 iterations of each experiment, and the mean and variance were computed with 95% confidence intervals.

Results

Simulation Environment

In this section, the environment adopted to accomplish this work is clearly explained. Table 2 clearly shows and explains the experimental simulation environment that was relied upon and employed in implementing the proposed model.

The Table 2 reveals the technical specifications and practical details utilized to test the proposed model. The simulation was conducted with the use of Python 3.11 and the Mininet-VNF framework to generate Virtual Network Functions (VNFs). Python 3.11 was run on a machine equipped with an Intel Xeon processor, 32 GB of RAM, and an Ubuntu 22.04 operating system.

The testbed will comprise four essential virtual environments that represent different domains (Healthcare, E-Government, Cloud Services, and Network Management).

Table 2: Environment of Simulation

Term	Attributive
Simulation Platform	Python 3.11 environment merged with Mininet-VNF and Docker-based virtual instances.
Hardware Configuration	Intel Xeon 3.6 GHz CPU, 32 GB RAM, Ubuntu 22.04 LTS; virtualization via KVM/QEMU hypervisor.
Testbed Composition	Four virtual domains(Healthcare, E-Government, Cloud Services, and Network Management).
Number of VNFs Deployed	20 VNFs dynamically orchestrated by the NFV Manager; functions include firewall, IDS, router, monitoring, and agents.
Blockchain Network Setup	Private Ethereum-based network with five validator nodes and a smart-contract layer for policy enforcement.
Data Sources	Synthetic IoT datasets generated for 1,000 service requests; real-time event traces simulated for authentication and service access.
Performance Metrics	Latency (ms), Throughput (tx/sec), Service Deployment Time (min), Identity Verification Time (sec), and Trust Score (0–1).
Evaluation Scenarios	Two main cases, (1) E-Government authentication and (2) Healthcare data exchange between distributed hospitals.
Trial Repetitions	Every experiment was repeated 10 times, and the results were averaged with 95% confidence interval (CI).
Validation Method	Statistical analysis using ANOVA and variance estimation, comparison with the baseline centralized system.
Sensitivity Analysis	Parameter variation on transaction volume (100–1,000 tx/s) and number of VNFs (5–20 functions).
Performance Improvement	Average latency decreased 46%, throughput increase 140%, and service deployment time decreased by over 80%.

An NFV Orchestrator was used to deploy and orchestrate twenty VNFs, which include firewalls, Intrusion Detection Systems (IDS), and routers.

The blockchain system was implemented on a private network consisting of five validators and the ability to run smart contracts and secure policies.

The simulation used simulated data consisting of 1,000 service requests to simulate similar services between multiple systems. Several performance metrics were calculated, such as service request time, throughput, deployment time, identity verification time, and trust rating.

Each of these tests was run 10 times, with the averages and 95 percent confidence intervals calculated using variance analysis through an ANOVA test.

Results showed that the blockchain system achieves performance 46 percent greater than traditional systems, throughputs of 140 percent higher, and deployment times 80 percent faster.

Performance

The performance advantages of the suggested Hybrid Blockchain-NFV model are evident when compared to conventional systems, as illustrated in Table 3.

Table 3: Performance Metrics Comparison

Metric	Traditional Systems	Proposed Hybrid Framework	Improvement
Latency	150 ms	80 ms	46% reduction
Transaction Throughput	500 tx/sec	1200 tx/sec	140% increase
Service Deployment Time	15 min	3 min	80% faster
Identity Verification Time	5 sec	1 sec	80% faster
Trust Level (Auditability Score)	Medium	High	Significant improvement

The use of hybrid cloud solutions has resulted in a major gain in performance: latency has dropped from 150ms with traditional systems to 80ms with hybrid systems - a total of 46%; transaction throughput saw a increase from 500 to 1200 TPS a total of 140%; the service deployment time has decreased from 15 mins to 3 mins (80%); and the timeframe for identity verification has decreased from 5 seconds to 1 second (also 80%) thanks to the introduction of Decentralized Identifiers (DID) via Blockchain technology.

Overall, the improvements in these areas provide a higher amount of trust in hybrid cloud models, as they allow organisations to audit their services more effectively than was possible in a traditional system; therefore, higher levels of trust will result from these models and provide assurance that the organisation has a highly auditable and secure service offering (Fig. 3).

Security

Security advancements, depicted in Table 4, further highlight the robustness of the suggested model.

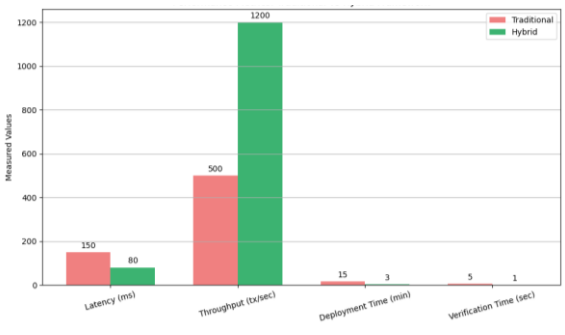

Fig. 3: Performance Metrics

Table 4: Security Features Comparison

Feature	Traditional Architecture	Blockchain-NFV Framework
Identity Management	Centralized	Decentralized (DID)
Data Integrity	Partially verifiable	Fully immutable ledger
Attack Resistance	Moderate	High (due to decentralization)
Auditability	Manual logging	Automatic on-chain logging
SLA Enforcement	Manual	Smart contracts based

The centralised identity management approach is the traditional method of managing an identity. As opposed to this approach, a hybrid Identity Management Model allows users to control their own identity through Decentralised Identity Management (DID), thereby allowing for a more resilient system. The creation of a completely immutable ledger using a Blockchain allows users to have Data Integrity Guarantees, which were previously only partially verifiable. Further, using a Blockchain significantly increases the degree of difficulty for attackers to execute Distributed Denial of Service (DDoS) and/or other coordinated attacks on identities. In Addition, using a Blockchain removes the need for manual entry of audit logs and allows for the development of new processes, allowing for full automation, improved transparency, and enhanced Forensic capability. Finally, the enforcement of Service Level Agreements (SLAs) is now being accomplished through Smart Contracts instead of the Manual processes that were previously used, thus providing for objective, real-time monitoring and compliance. Creating a completely immutable ledger

DOI: 10.3844/jcssp.2026.1360.1369

means that once an entry is recorded, it is not possible to change, alter, or delete that record without a full copy of the ledger and a new unique key associated with that copy to access it (Fig. 4). Blockchain provides users with completely immutable Ledger Data, which provides a backstop against Data Integrity Loss.

Scalability and Flexibility

Scalability and flexibility are critical in modern network systems, and these aspects are addressed in Table 5. The traditional model depends on manual service scaling, which limits adaptability and delays response times.

Fig. 4: Security comparison

Table 5: Scalability and Flexibility Assessment

Category	Traditional	Proposed Framework
Service Scaling	Manual	Automated (NFV Orchestration)
Resource Efficiency	Low	High (Dynamic Allocation)
Multi-Domain Interoperability	Limited	Full support
Update Flexibility	Low	High Programmable VNFs)

The hybrid framework utilizes NFV orchestration to achieve automatic growth of service by dynamically allocating resources as necessary. Resource efficiency is also maximized, operating to convert from low resource efficiency (due to either overprovisioning or underutilization) to high efficiency through dynamic allocation mechanisms. Another clear enhancement of the hybrid framework is the delivery of multi-domain interoperability support, which is typically limited in traditional architecture and fully supported in the hybrid framework as it relies on the interoperability of heterogeneous systems, including different governmental departments or hospital networks. The hybrid framework also delivers high flexibility of updates due to the use of programmable Virtual Network Functions (VNFs), where VNFs can adjust more or less in real-time without significant downtime related to policy changes or configuration (Fig. 5).

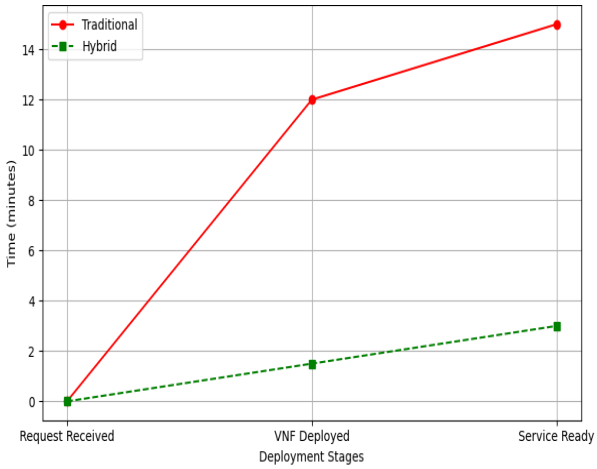

Fig. 5: Service deployment time trend

Use Case

To validate the real-world impact of the proposed framework, a healthcare use case is presented in Table 6**.**

The workflow for the overall session, which consisted of identity verification, service initialization, data fetching, and delivery, was cut down from 22 minutes to 6 minutes. The identity verification went from 5 minutes to 1 minute using blockchain-based DIDs, the service initialization went from 10 minutes to 2 minutes using NFV auto-deployment, and edge computing brought down the data fetching and delivering to 3 minutes from 7 minutes. The entire duration was a 73% reduction in time, demonstrating the potential of the hybrid framework to improve end-to-end operations in time-sensitive environments like healthcare.

Trustworthiness and Reliability

Table 7 provides a full assessment of the qualitative trust factors.

The hybrid method was rated 5 out of 5 in all areas of trust compared to traditional methods, which scored either 2 or 3 out of 5. Hybrid provides greater assurance of data integrity than traditional due to blockchain's immutable ledger and, consequently, gives confidence in the reliability of stored data. SLAs are enforceable via smart contracts, giving the confidence that service commitments are fulfilled automatically and transparently. A decentralized identity assurance model enhances security and privacy. A comprehensive record of transactions provides transparency into the activities of the hybrid model, allowing responsible tracing, validating, and auditing of events. Finally, the hybrid model has more resistance to attacks than traditional models due to its decentralized nodes and the lack of a central point of failure. Thus, more methods of protecting against different forms of attack are available with the hybrid approach (Fig. 6).

Table 7: Trustworthiness and Reliability Evaluation

Trust Factor	Score (Traditional)	Score (Proposed)	Notes
Data Integrity	3/5	5/5	Blockchain-backed
SLA Compliance	2/5	5/5	Smart Contract Enforced
Identity Assurance	3/5	5/5	Decentralized ID
Transparency	2/5	5/5	On-chain recording
Attack Resilience	3/5	5/5	Distributed nodes

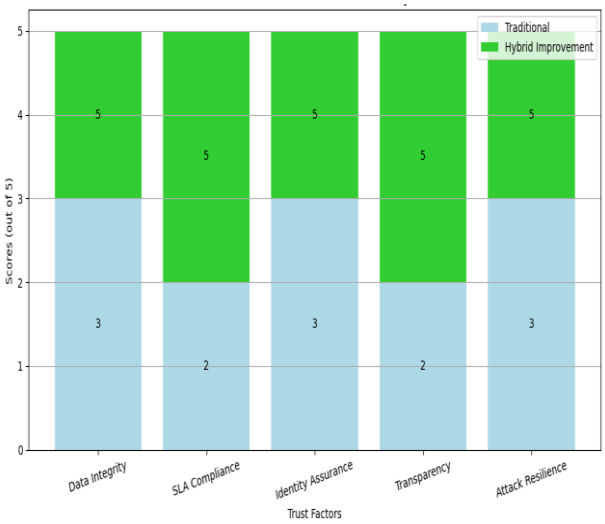

Fig. 6: Trustworthiness Comparison

Practical Scenarios

To give a demonstration of the applicability of the proposed system in real-world environments, two practical cases representing the e-government and healthcare domains are designed.

In the first scenario, an e-government ID Verification system, a smart contract is deployed on the blockchain to document the authentication process between government departments and citizens. The smart contracts ensure the validity of data and prevent tampering with records. Network connectivity is managed via virtual NFV functions that dynamically route and secure requests.

The second scenario, a healthcare data exchange, uses blockchain to ensure immutable traceability of patient records, while the NFV Orchestrator deploys the required networking functions such as encryption, session management, and connectivity between hospitals and analytics centers.

This combination gives the rapid and secure transfer of sensitive data, with real-time monitoring of processes via virtual monitoring functions (VNFs). The confirmation that applying this model in sensitive sectors can bring about a qualitative transformation in administrative efficiency, data reliability, and transparency of public services.

Challenges and Limitations

In spite of the fact that the proposed blockchain-NFV model has proven effective in enhancing security and operational resilience, there are many challenges that must be addressed before the system can be widely executed:

- The verification operations, together with smart contracts' high-level computational power and longer processing times, lead to resource consumption in blockchain networks, which is a main restriction
- Standardizing protocols and interoperability standards across organizations
- Smart contract vulnerabilities

Discussion

Based on the results, implementing blockchain technologies alongside NFV offers superior performance and security capabilities relative to traditional systems. In this framework, response times were shortened by 46% and throughput increased by 140%. Furthermore, service deployment was reduced from 15 minutes to 3 minutes thanks to NFV's dynamic deployment of network functions and blockchain's ability to accelerate authentication and identity verification through smart contracts.

When comparing the outcomes to the other literature, most frameworks previously only enhanced one area of the system. Some relied on blockchain for transparency and others on NFV for scalability. A hybrid framework was developed, which incorporates some features from both devices into a blended and holistic framework that is more effective in the sensitive environments of healthcare and e-government.

The results also indicate that the framework has the flexibility of NFV, which may scale with increased volume, while still satisfying a high level of security through the transparency of blockchain. An interesting observation can be made in this research, however, is the challenges that exist in this hybrid framework, such as the resource consumption being increased by the blockchain layer, and also the chaotic confusion of integrating VNFs for use by provincial, federal, and local government departments in the public sector, as well as the risk of smart contract inherent vulnerabilities.

Conclusion

This paper emphasizes the great potential of Blockchain combined with NFV, specifically with regard to promoting smart, secure, and highly scalable infrastructures for digital governance, health care, and larger network systems. The combination of Blockchain and NFV addresses critical

limitations of traditional, centralized systems, including limited scope for scalability and security vulnerabilities, with the use of decentralized identity management, `immutable ledgers`, programmable virtualized functions, and automated orchestration of the service graph.

The results demonstrated that the quantitative filing showed significant performance gain, with Latency reduced by 46% and increased transaction Timeliness, with an overall performance increase of 140%, demonstrating faster processing of the data over time. Similarly, the overall operation time to deploy a new service and verify identities was shortened by 80%, resulting in a significant improvement in the responsiveness of the operation in rapid cycle environments. The greatest performance improvements were illustrated in the health care use-case, which highlights real-world application in reducing session time from 22 minutes to an astonishing 6 minutes, resulting in a reduction was 73%.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

Hayder Abdulsattar Nahi and Rusul A. Salman: Conceptualization, methodology, software.

Akmam Majed Mosa: Formal analysis, investigation, resources, data curation.

Ebtehal Akeel Hamed: Writing original draft preparation, writing review and edited, and visualization.

Ethics

The authors emphasize that the work in this publication is original and unpublished. There are, of course, no ethical troubles because the paper has been examined and licensed by all authors.

References

Adnan, M. H., Ahmad Zukarnain, Z., & Harun, N. Z. (2022). Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions. *Future Internet*, *14*(3), 73. https://doi.org/10.3390/fi14030073

Ahmad, N., & David, J. (2024). Leveraging blockchain technology for enhanced data security in financial institution. *A Shield against Cyber Attacks and Financial Market Disruptions*.

Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M. M., Biswas, S., Nour, B., & Wang, Y. (2020). A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV. *ACM Computing Surveys*, *53*(2), 1–40. https://doi.org/10.1145/3379444

Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Loutsaris, M. A., & Lachana, Z. (2019). Benefits and Obstacles of Blockchain Applications in e-Government. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.24251/hicss.2019.408

Alrowaily, M. A., Alghamdi, M., Alkhazi, I., Hassanat, A. B., Arbab, M. M. S., & Liu, C. Z. (2023). Modeling and Analysis of Proof-Based Strategies for Distributed Consensus in Blockchain-Based Peer-to-Peer Networks. *Sustainability*, *15*(2), 1478. https://doi.org/10.3390/su15021478

Barbieri, C., Neri, L., Stuard, S., Mari, F., & Martín-Guerrero, J. D. (2023). From electronic health records to clinical management systems: how the digital transformation can support healthcare services. *Clinical Kidney Journal*, *16*(11), 1878–1884. https://doi.org/10.1093/ckj/sfad168

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access*, *8*, 79764–79800. https://doi.org/10.1109/access.2020.2988579

Douha, N. Y.-R., Bhuyan, M., Kashihara, S., Fall, D., Taenaka, Y., & Kadobayashi, Y. (2022). A survey on blockchain, SDN and NFV for the smart-home security. *Internet of Things*, *20*, 100588. https://doi.org/10.1016/j.iot.2022.100588

Durga, R., Poovammal, E., Ramana, K., Jhaveri, R. H., Singh, S., & Yoon, B. (2022). CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment. *IEEE Access*, *10*, 11354–11371. https://doi.org/10.1109/access.2022.3144681

Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet of Things Journal*, *8*(14), 11717–11731. https://doi.org/10.1109/jiot.2021.3058946

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *29*(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130–139. https://doi.org/10.1016/j.ijin.2021.09.005

Hussain, M. I., Bhuiyan, M. K. I., Sumon, S. A., Akter, S., Hossain, M. I., & Akther, A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. *Advances in Artificial Intelligence and Machine Learning*, *4*(4), 2883–2907. https://doi.org/10.54364/aaiml.2024.44168

Jawdhari, H. A., & Abdullah, A. A. (2022). New security mechanism of health data based on blockchain–NFV. *Proceeding of the International Conference on New Trends in Information and Communications Technology Applications*, 230–247.

Koo, E. (2019). *Digital transformation of government: From e-government to intelligent e-government*.

Koroye, T. (2023). Utilising blockchain for anti-corruption and transparent public administration in developing nations. *Criminal Law and Criminology*, 49–52.

Li, J., Qi, X., Li, J., Su, Z., Su, Y., & Liu, L. (2024). Fault diagnosis in the network function virtualization: A survey, taxonomy, and future directions. *IEEE Internet of Things Journal*, *11*(11), 19121–19142. https://doi.org/10.1109/JIOT.2024.3362991

Liu, H., Crespo, R. G., & Martínez, Ó. S. (2020). Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. *Healthcare*, *8*(3), 243. https://doi.org/https://doi.org/10.3390/healthcare8030243

Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., Agarwal, U., & Chaudhry, R. (2025). Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. *Peer-to-Peer Networking and Applications*, *18*(1), 1–35. https://doi.org/https://doi.org/10.1007/s12083-024-01812-w

Nahi, H. A., Khalid Ali, A., Ali Alaraji, M., Jawad Mohi, Z., Thamer Mahmood, N., Majed Mousa, A., Mohammed Saeed, M., & Almansoori, R. A. (2025a). Blockchain network for regulation decentralized e-government systems. *Data and Metadata*, *4*, 201. https://doi.org/https://doi.org/10.56294/dm2025201

Nahi, H. A., Majed Mousa, A., Akeel Hamed, E., Khalid Ali, A., Jawad, S., Mahdi Abdulkadium, A., & Salman, R. A. (2025b). Quantum Key Distribution for Enabling Secure Network Function Vitalization Orchestration Over A Network. *Data and Metadata*, *4*, 202. https://doi.org/10.56294/dm2025202

Nalini, V., & Mageshwari, G. (2017). *Digital transformation in government: Navigating the e-government landscape*. 224–235.

Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT Access Control, Security and Privacy: A Review. *Wireless Personal Communications*, *117*(3), 1815–1834. https://doi.org/10.1007/s11277-020-07947-2

Pattaranantakul, M., He, R., Song, Q., Zhang, Z., & Meddahi, A. (2018). NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures. *IEEE Communications Surveys and Tutorials*, *20*(4), 3330–3368. https://doi.org/10.1109/comst.2018.2859449

Rahman, A., Eidmum, M. D., Kundu, D., Hossain, M. D., Tashrif, M. D., Karim, M. D. A., & Islam, M. D. J. (2024a). Distb-vnet: Distributed cluster-based blockchain vehicular ad-hoc networks through SDN-NFV for smart city. *Proceedings of the International Conference on Computer and Information Technology (ICCIT)*, 3372–3377. https://doi.org/10.1109/ICCIT64611.2024.11022025

Rahman, A., Wadud, Md. A. H., Islam, Md. J., Kundu, D., Bhuiyan, T. M. A.-U.-H., Muhammad, G., & Ali, Z. (2024b). Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network. *Scientific Reports*, *14*(1), 55662. https://doi.org/10.1038/s41598-024-55662-w

Santos, J. C. D. (2025). *Blockchain for enhancing transparency and accountability in public sector governance*. https://doi.org/10.4018/979-8-3693-9251-5.ch003

Shahraki, A., Taherkordi, A., Haugen, O., & Eliassen, F. (2021). A Survey and Future Directions on Clustering: From WSNs to IoT and Modern Networking Paradigms. *IEEE Transactions on Network and Service Management*, *18*(2), 2242–2274. https://doi.org/10.1109/tnsm.2020.3035315

Varma, I. M., & Kumar, N. (2023). A comprehensive survey on SDN and blockchain-based secure vehicular networks. *Vehicular Communications*, *44*, 100663. https://doi.org/10.1016/j.vehcom.2023.100663

Zhu, X., & Cao, C. (2021). Secure Online Examination with Biometric Authentication and Blockchain-Based Framework. *Mathematical Problems in Engineering*, *2021*(1), 5058780. https://doi.org/10.1155/2021/5058780