# Blockchain-Based Secure DNS System

**Harshitha Thottempudi, Fan Li, PhD, Assistant Professor**

**Department of Math and Computer Science, College of Arts & Science**

## ABSTRACT

This project presents a Blockchain-Based Secure Domain Name system (DNS) that addresses the critical vulnerability in traditional DNS infrastructure where records can be silently modified without any proof of tampering. Every DNS record is secured through SHA-256 cryptographic hash chaining and permanently anchored on the Solana blockchain providing tamper-evident and publicly verifiable DNS record management.

## INTRODUCTION

Traditional DNS suffers from DDoS (Distributed Denial-of-service) attacks and cache poisoning due to its centralized architecture which lacks transparency in handling record changes. The 2019 Sea Turtle attack hijacked DNS records of government organizations across 13 countries going undetected for months motivating the need for tamper-evident DNS.

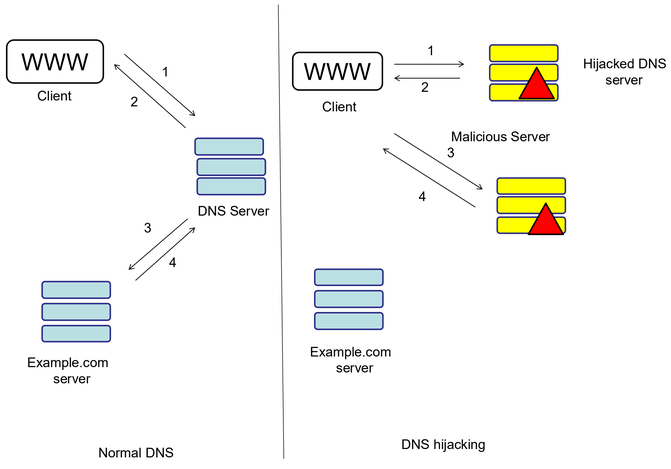


Fig.1 This shows how DNS server works when it in normal state and DNS is hijacked by the attacker

Solana is faster and cheaper which is essential for anchoring high frequency DNS record operations permanently on-chain without smart contracts

Table 1 Ethereum vs Solana

| Property | Ethereum | Solana |
|---|---|---|
| Speed | 15 TPS | 65,000 TPS |
| Cost/tx | $5–$50 | $0.00025 |
| Confirmation | 15–30 sec | <1 sec |
| Smart contract | Yes | Not need |

## METHODS

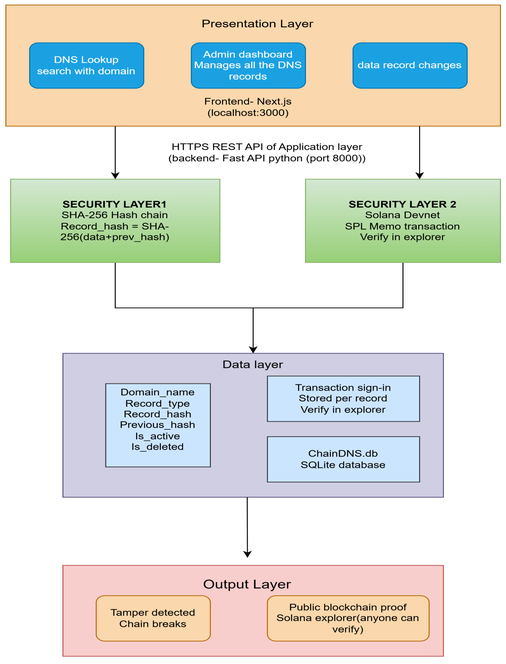


Fig. 2 Blockchain based DNS architecture

SHA-256 hash computed using current record data combined with previous record hash. Any modification immediately breaks the chain at exact point of tampering. Deleted records preserved permanently, they are never removed from chain.

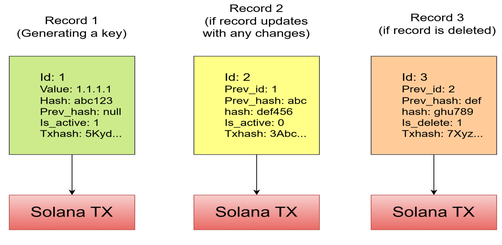


Fig. 3 How every record is stored as a timestamp on blockchain

Every DNS operation writes a permanent SPL (Solana program library) Memo transaction to Solana containing domain name, operation type, and SHA-256 hash.

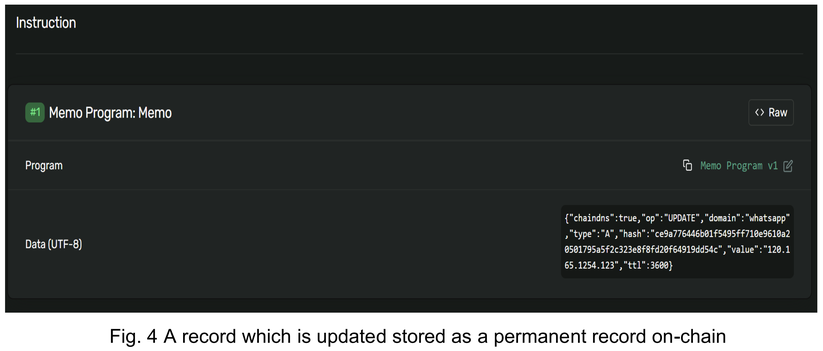


Fig. 4 A record which is updated stored as a permanent record on-chain

## RESULTS

1. SHA-256 hash chain successfully secured DNS records with instant tamper detection and 100% chain integrity verified across all operations.
2. Dual-layer security combining local hash chaining and public blockchain anchoring successfully detected and preserved evidence of every unauthorized modification attempt.

Table 2 Traditional DNS vs BDNS

| Feature | Traditional DNS | BDNS (Blockchain-based Domain Name System) |
|---|---|---|
| Tamper detection | X | ✓ |
| Public verification | X | ✓ |
| Audit trail | X | ✓ |
| Record integrity | ✓ | ✓ |
| Immutability | X | ✓ |

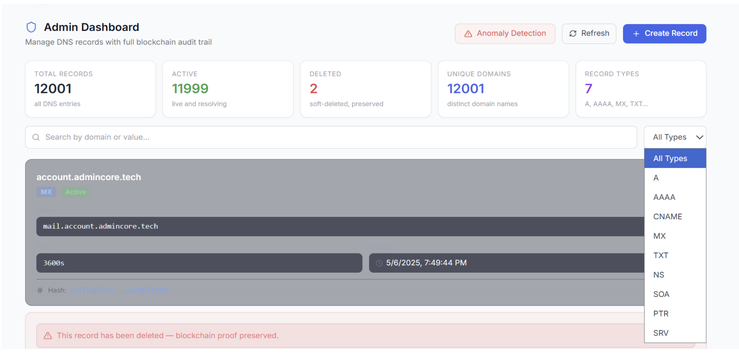


Fig. 5 This shows record types, total records, record status

## CONCLUSION

This project successfully demonstrates that blockchain immutability principles can be practically applied to DNS infrastructure. ChainDNS addresses the fundamental security gap in traditional DNS by combining SHA-256 hash chaining with Solana blockchain anchoring, providing tamper-evident and trustless DNS record verification at minimal cost.

## FUTURE WORK

1. Integrate a hybrid machine learning based anomaly detection model to monitor live DNS traffic in real time identifying suspicious activity automatically.
2. Implement automatic alert notifications when hash chain integrity breaks enabling immediate administrator response.

## REFERENCES

1. Juseong Jeon, Sejin ParK, A Survey on Traditional DNS and Blockchain-Based DNS: Comparative Analysis, Challenges, and Future Directions.
2. Zecheng Li; Shang Gao; Zhe Peng; Songtao Guo; Yuanyuan Yang; Bin Xiao, B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology, IEEE Transactions on Network Science and Engineering
3. Salima Omar, Asri Ngadi, Hamid H. Jebur, Machine learning techniques for anomaly detection: an overview, International Journal of Computer Applications (0975 – 8887) Volume 79 – No.2, October.