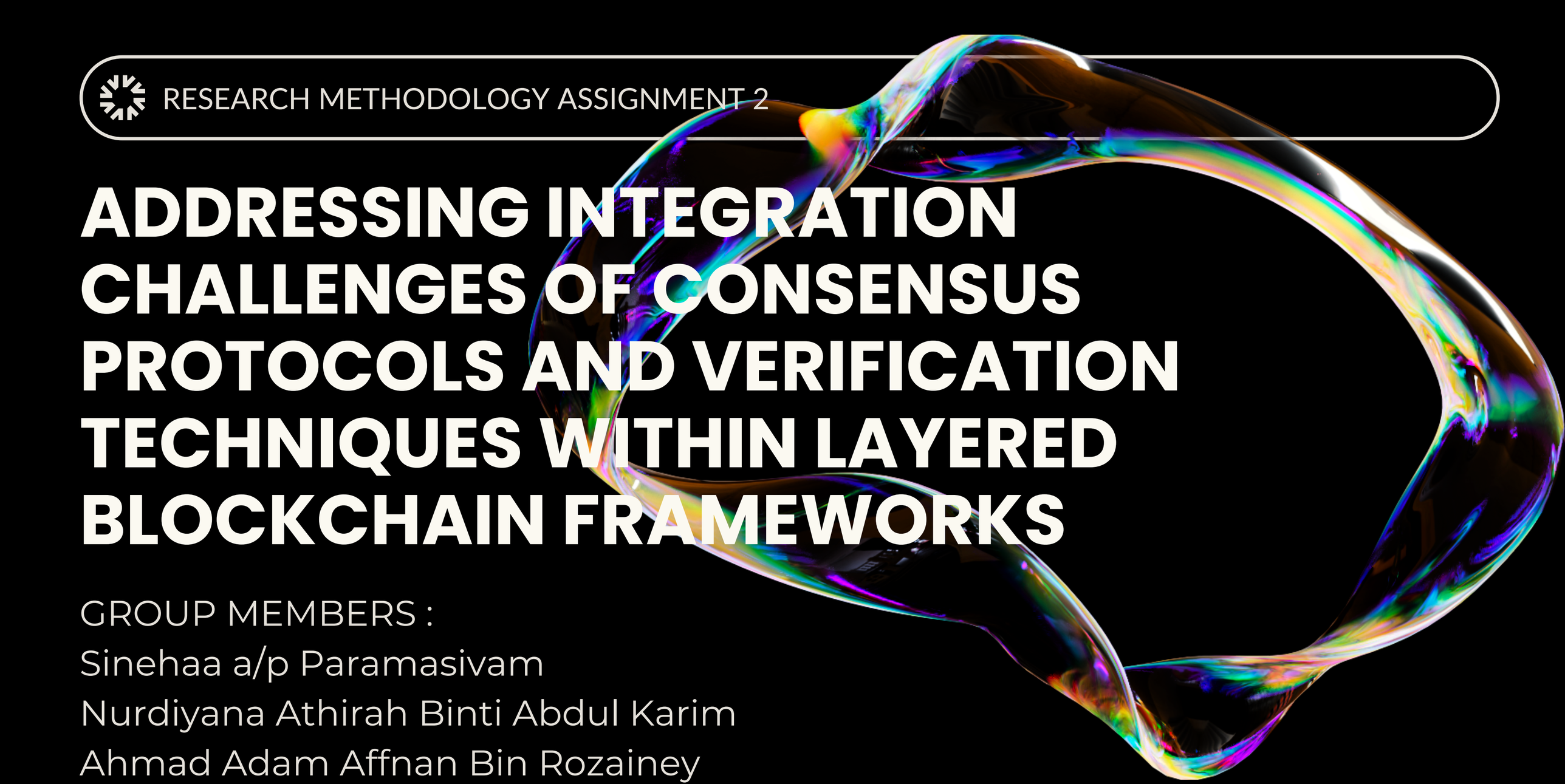
RESEARCH METHODOLOGY ASSIGNMENT 2

ADDRESSING INTEGRATION CHALLENGES OF CONSENSUS PROTOCOLS AND VERIFICATION TECHNIQUES WITHIN LAYERED BLOCKCHAIN FRAMEWORKS



GROUP MEMBERS :
Sinehaa a/p Paramasivam
Nurdiyana Athirah Binti Abdul Karim
Ahmad Adam Affnan Bin Rozainey
Karthekeyan

EXECUTIVE SUMMARY

Blockchain Vulnerabilities

- Rapid evolution of blockchain brings sophisticated threats.

Research Focus

- Unified blockchain security framework.
- Integration of Proof of Adjourn (PoAj) and verification methods.
- Quantum-resistant cryptography.

Outcome

- Enhanced resilience against cyber threats.

PROBLEM STATEMENT

Key Issues:

- Fragmented consensus protocols and formal verification techniques.
- Lack of integration in multi-layered blockchain frameworks.
- Rising threats like quantum computing.

Why It Matters

- Without addressing these issues, blockchain systems remain vulnerable, potentially risking data integrity across industries.

RESEARCH QUESTIONS

HOW

How can consensus protocols and verification techniques be integrated into a multi-layer blockchain framework?

WHAT

What are the scalability challenges when integrating new protocols like PoAj?

HOW

How can the blockchain framework address threats from quantum computing?

RESEARCH OBJECTIVES

OBJECTIVE 1

Develop an integrated blockchain security framework combining PoAj and formal verification.

OBJECTIVE 2

Evaluate scalability and implementation challenges in real-world blockchain environments

OBJECTIVE 3

Investigate quantum-resistant cryptographic techniques for future-proofing blockchain.

HYPOTHESES

H1

Integrated consensus and verification methods reduce security risks.

H2

Quantum-resistant cryptography strengthens blockchain systems against quantum attacks.

H3

Combining PoAj and formal verification can maintain high performance under transaction-heavy conditions.

JUSTIFICATION/MOTIVATION

Relevance in Recent Years

- Blockchain systems are expanding and scaling rapidly.
- Fragmented security approaches have exposed vulnerabilities.
- Integrating layered frameworks with innovative consensus protocols (e.g., PoAj) and formal verification methods is crucial for enhancing system resilience.

Emerging Threats

- Quantum computing and advanced technologies pose significant future risks.
- Addressing integration challenges in blockchain security is vital to defend against increasingly sophisticated cyber threats.

LITERATURE REVIEW

1. Blockchain Security Research

- Ongoing research focuses on improving security.
- Key areas: consensus protocols, formal verification, and security frameworks.
- Challenge: fragmented approach in integrating these components.

2. Multi-Layered Security Architectures

- Flexible architectures to secure different blockchain elements.
- Theoretical strength, but scalability and real-world applicability are uncertain.

3. Formal Verification Techniques

- Crucial for detecting vulnerabilities.
- Limited studies on broader use within multi-layered systems.
- High computational demands raise concerns about adaptability.

LITERATURE REVIEW

4. Quantum Computing Threat

- Quantum computing threatens current encryption methods.
- Quantum-resistant cryptographic approaches suggested, but lack real-world testing in blockchain systems.

5. Consensus Protocols (e.g., Proof of Adjourn)

- Proposed to improve scalability and energy efficiency.
- Lack of studies on practical implementation and integration with other security mechanisms.

6. Identified Research Gap

- Lack of integration across blockchain security solutions.
- Focus on isolated aspects without a unified, multi-layered system.
- This fragmentation limits scalability and exposes systems to new threats.

RESEARCH METHODOLOGY

COMPREHENSIVE LITERATURE REVIEW

- Identify existing frameworks
- Highlight research gaps

FRAMEWORK DESIGN AND DEVELOPMENT

- A layered blockchain integration framework will be designed.
- Consensus protocols
- Verification techniques

CONTROLLED ENVIRONMENT TESTING

- Consensus Protocol: Proof of Work (PoW), Proof of Stake (PoS), Proof of Adjourn (PoAj)
- Verification Technique
- Quantum-Resistant Methods

SIMULATED QUANTUM ATTACKS

- Quantum-resistant cryptography will be subjected to simulated quantum attacks using post-quantum cryptographic techniques.

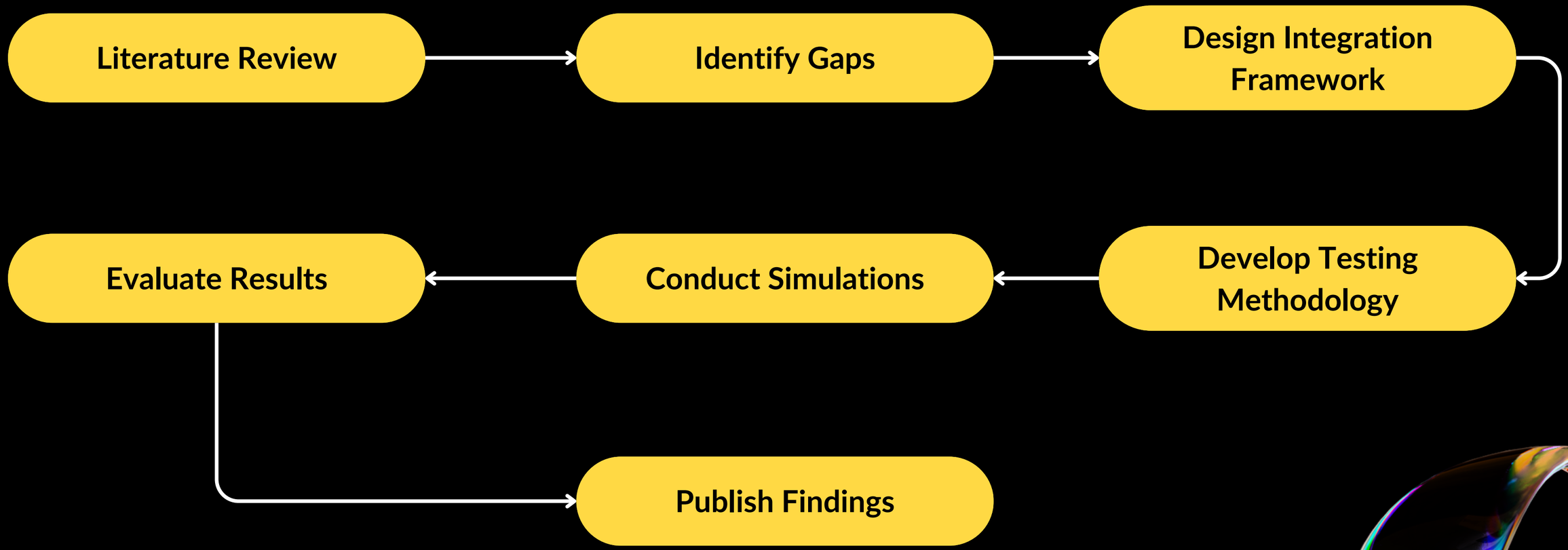
DATA COLLECTION AND METRICS

- Scalability
- Security
- Efficiency
- Resilience

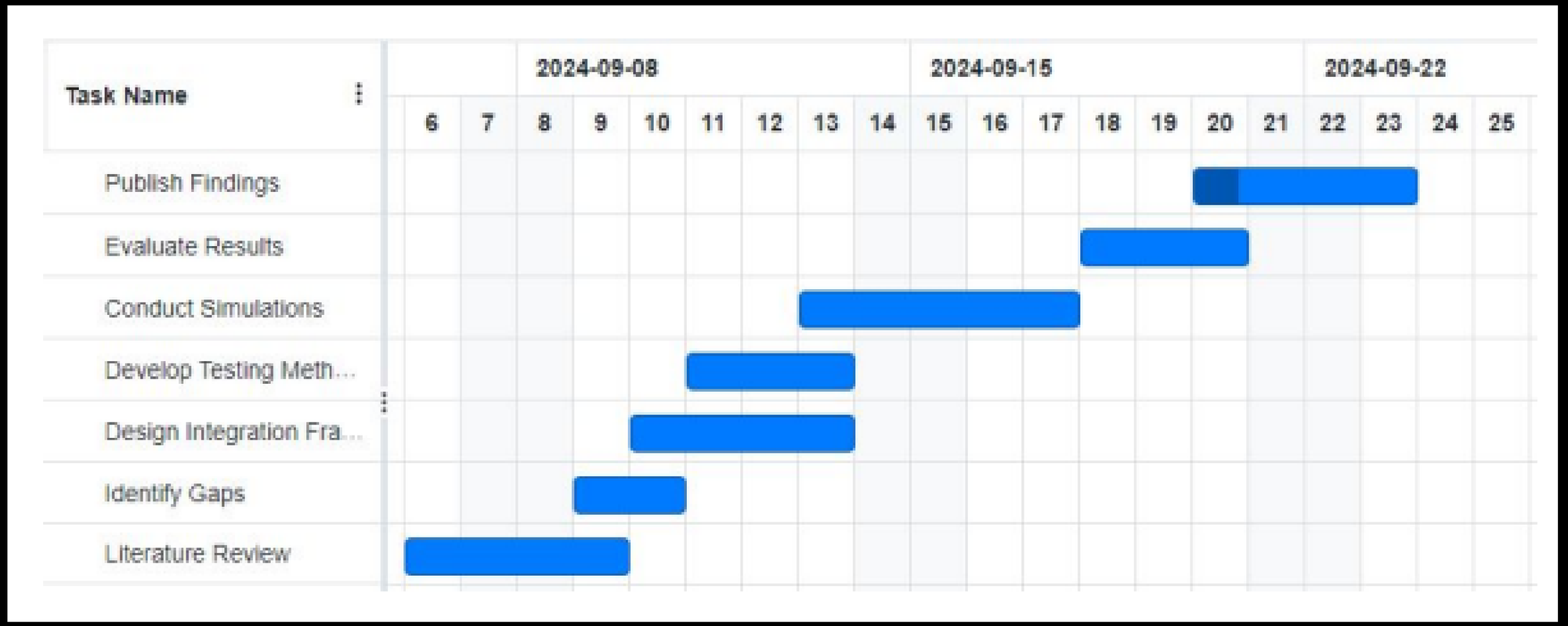
DATA ANALYSIS

- Quantitative Data: Metrics from the performance analysis will be evaluated.
- Qualitative Feedback: Insights from testing environments will reveal any practical challenges

RESEARCH FINDINGS (ACTIVITIES)



RESEARCH FINDINGS(SCHEDULE)



EXPECTED RESULTS & IMPACT

NOVEL THEORIES & FINDINGS

- Improved Integration Framework
- Quantum-Resistant Cryptography
- Evaluation Metrics

IMPACT ON SOCIETY

- Increased Trust & Security
- Empowerment

IMPACT ON THE NATION

- Strengthening National Security
- Supporting Innovation

ECONOMIC IMPACT

- Economic Growth
- Job Creation

REFERENCES

- Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H.-N. (2022). Systematic review of security vul nerabilities in ethereum blockchain smart contract. IEEE Access, 10, 6605–6621. doi: 10.1109/ac cess.2021.3140091
- Marijan, D., & Lal, C. (2022). lenges, and research directions. Blockchain verification and validation: Techniques, chal Computer Science Review, 45, 100492. Retrieved from https://www.sciencedirect.com/science/article/pii/S1574013722000314 doi: https://doi.org/10.1016/j.cosrev.2022.100492
- Rifat Hossain, M., Nirob, F. A., Islam, A., Rakin, T. M., & Al-Amin, M. (2024). A comprehensive analysis of blockchain technology and consensus protocols across multilayered framework. IEEE Access, 12, 63087-63129. doi: 10.1109/ACCESS.2024.3395536
- Sayeed, S., & Marco-Gisbert, H. (2020, 09). Proof of adjourn (poaj): A novel approach to mitigate blockchain attacks. Applied Sciences, 10, 6607. doi: 10.3390/app10186607

CONCLUSION

The report concludes that integrating consensus protocols, formal verification techniques, and quantum-resistant cryptography into a cohesive layered blockchain framework is essential for improving security and scalability. By addressing the fragmented nature of current blockchain security solutions, the proposed framework can enhance resilience against emerging threats, including quantum computing. The findings offer valuable insights for developers, researchers, and policymakers, and the framework is expected to contribute to broader adoption of blockchain technology by increasing trust, national security, and economic growth through innovation and job creation.

Q & A

for your time and attention