ITEC312

2025 PLAN + Explanation presentation

What is Quantum Guard AI?

- Quantum Guard AI is a cloud-based, AI-powered blockchain fraud detection system designed to serve financial institutions. It monitors transactions, flags suspicious behaviour, and explains risk scores using explainable AI (XAI). It is future-proofed for quantum security standards and aims to support financial compliance at scale.

- Quantum Guard AI is designed to be your comprehensive solution for blockchain and financial transaction analysis, combining cutting-edge security with powerful AI capabilities to help you detect risks and understand transaction patterns effectively

Team roles project

Liam – Lead software engineer, Scrum master

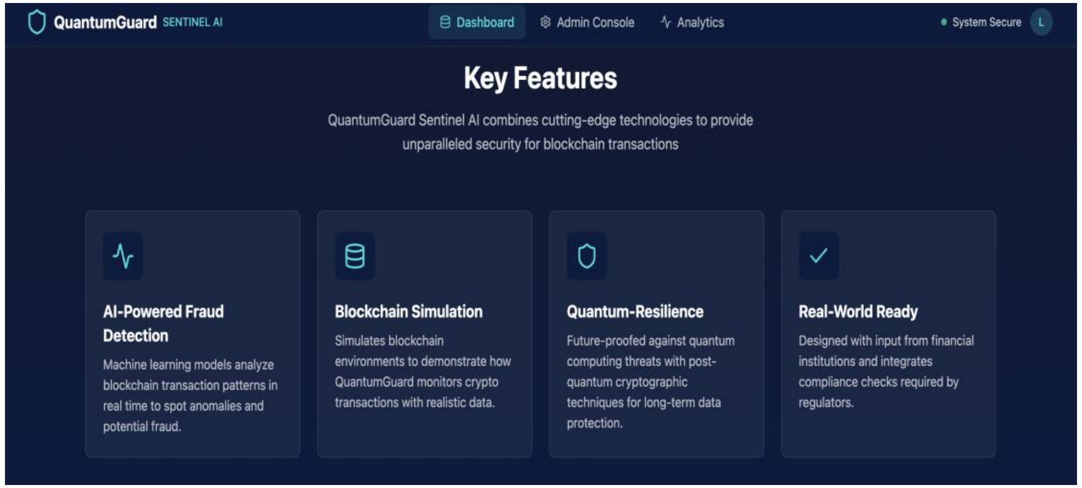
Lucas – Testing/Regulation Project manager, Co developer

Tuong- Business development manager, AI/architecture research analyst

Quantum Guard AI Features

1. 🧠 AI-Powered Intelligence

- Natural Language Search - Ask questions about your data in plain English using Open AI GPT-4o
- Advanced Multimodal Analytics - Combines clustering, behavioural analysis, and network insights
- Predictive Analysis - Forecasts future transaction trends, risk levels, and anomaly likelihood
- AI-Generated Insights - Smart recommendations based on transaction patterns



Key Features

QuantumGuard Sentinel AI combines cutting-edge technologies to provide unparalleled security for blockchain transactions

AI-Powered Fraud Detection

Machine learning models analyze blockchain transaction patterns in real time to spot anomalies and potential fraud.

Blockchain Simulation

Simulates blockchain environments to demonstrate how QuantumGuard monitors crypto transactions with realistic data.

Quantum-Resilience

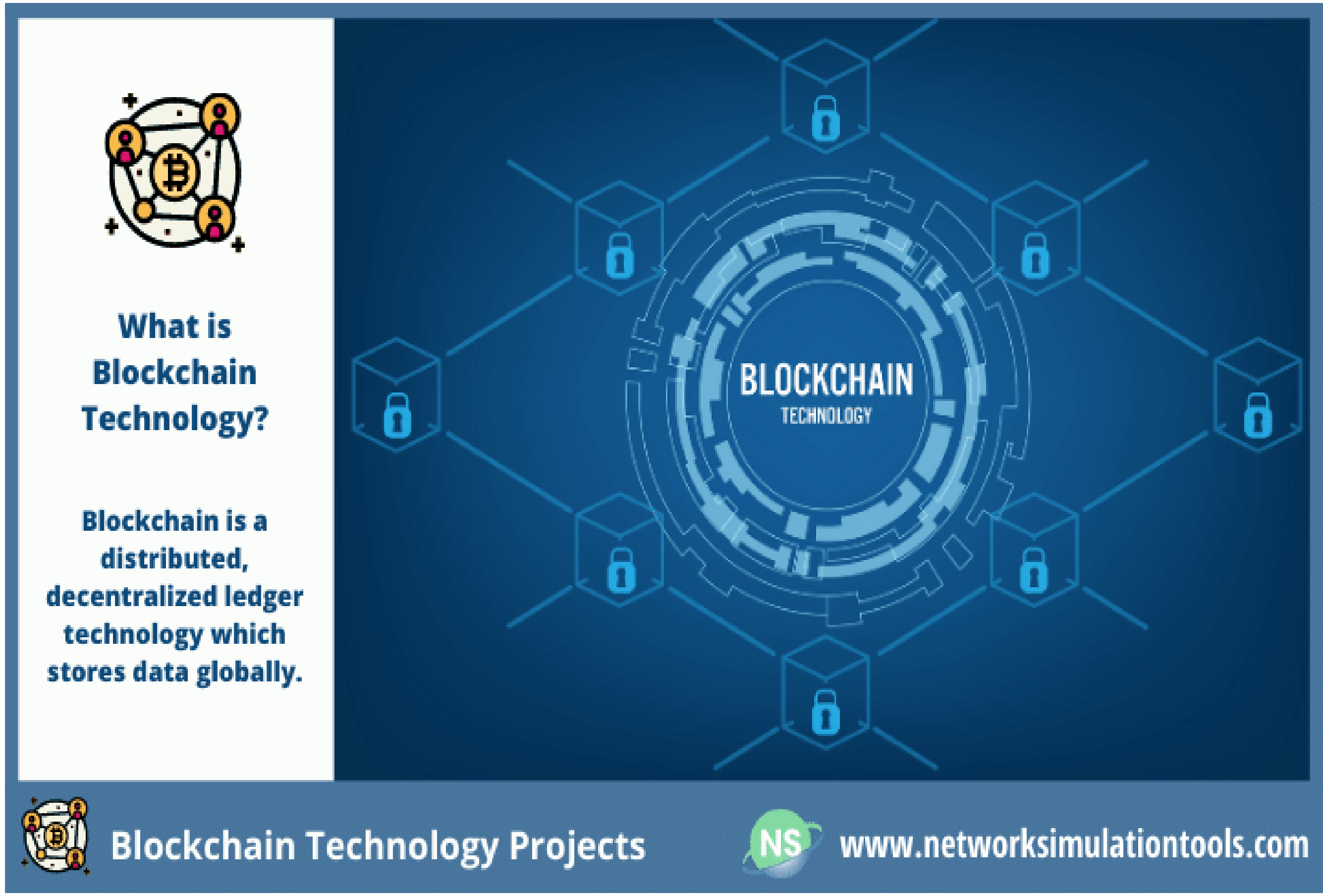
Future-proofed against quantum computing threats with post-quantum cryptographic techniques for long-term data protection.

Real-World Ready

Designed with input from financial institutions and integrates compliance checks required by regulators.

2. 📊 Blockchain Transaction Analysis

- Multi-Format Support - Handles blockchain transactions (Ethereum, Bitcoin) and traditional banking data
- Real-Time Processing - Instant analysis of uploaded transaction datasets
- Risk Assessment - Intelligent scoring system to identify potentially suspicious transactions
- Anomaly Detection - Machine learning algorithms to spot unusual transaction patterns



What is Blockchain Technology?

Blockchain is a distributed, decentralized ledger technology which stores data globally.

Blockchain Technology Projects

www.networksimulationtools.com

3. Quantum-Resilience

🔐 Core Security
Post-Quantum Cryptography - Advanced encryption to protect sensitive transaction data against future quantum threats
Secure Data Processing - All analysis happens with encrypted data protection as well as

Primary functions:

-Transaction security

-AUSTRAC reporting protection

-inter-bank communication

Quantum Guard AI isn’t just a catchy name it reflects a commitment to security against emerging threats. As government agencies warn that current cryptography (RSA, ECDSA, etc.) could be broken by quantum computers by 2030. Our solution plans to incorporate **post-quantum cryptography** and quantum-safe practices. This ensures long-term protection of sensitive financial data, giving adopters a competitive edge in security.

Additional features -Quantum Guard AI

📈 Visualizations

- Interactive Network Maps - See transaction flows and connections between addresses
- Risk Heatmaps - Visual representation of risk distribution across transactions
- Timeline Analysis - Track transaction patterns over time
- Anomaly Visualization - Highlight unusual transactions in your dataset

💾 Data Management

- Database Integration - Save and retrieve analysis sessions for future reference
- Export Capabilities - Download results as CSV or Excel files
- Session Management - Load previous analyses and compare results
- Converter Tools - Built-in support for Etherscan and other blockchain data formats

🎯 Specialized Features

- Money Laundering Detection - Identifies patterns commonly associated with financial crimes
- Network Analysis - Understands relationships and flows between addresses
- Customizable Thresholds - Adjust risk and anomaly sensitivity to your needs
- Multi-Dataset Analysis - Compare and analyse multiple transaction sets

🚀 Advanced Analytics

- Transaction Clustering - Groups similar transactions for pattern recognition
- Behavioural Pattern Analysis - Identifies user behaviour trends and anomalies
- Volume & Value Forecasting - Predicts future transaction volumes and values
- Risk Trend Prediction - Anticipates future risk levels and monitoring needs

Quantum Guard AI Fraud Classification

What Quantum Guard AI Considers "Fraud"

Quantum Guard AI uses multiple indicators to classify transactions as potentially fraudulent:

- 📊 Risk Score Calculations
- High Transaction Values - Unusually large amounts compared to typical patterns
- Frequency Anomalies - Rapid succession of transactions or unusual timing
- Address Patterns - New or suspicious wallet/account addresses
- Behavioural Deviations - Transactions that don't match historical user behaviour

🔍 Anomaly Detection Criteria

- Statistical Outliers - Transactions that fall outside normal distribution patterns
- Network Anomalies - Unusual connection patterns between addresses
- Time-based Anomalies - Transactions at unusual hours or frequencies
- Value Distribution Anomalies - Amounts that don't fit typical spending patterns

⚖️ Machine Learning Indicators

- Clustering Analysis - Transactions that don't fit into normal behavioural clusters
- Pattern Recognition - Sequences that match known fraudulent patterns
- Risk Correlation - Multiple risk factors occurring together

🎯 Specific Fraud Patterns

- Rapid Account Draining - Quick successive withdrawals
- Round Number Transactions - Suspicious even amounts (often automated)
- Cross-Border Anomalies - Unusual geographic transaction patterns
- Velocity Checks - Too many transactions in short time periods

📈 Risk Threshold Impact

- 0.7+ Risk Score = Flagged as high-risk/potentially fraudulent
- Anomaly Detection = Transactions that deviate significantly from normal patterns
- Combined Indicators = Multiple risk factors increase fraud likelihood

🔄 Dynamic Assessment

- The system continuously learns from transaction patterns and adjusts its fraud detection based on:
- Historical transaction behaviour
- Network relationship analysis
- Value and timing pattern analysis
- Cross-reference with known fraud indicators
- Note: Quantum Guard AI provides risk assessment and anomaly detection - the final determination of actual fraud requires human review and investigation of flagged transactions.

Quantum Guard AI Skills Learnt

🎓 Skills Learnt Through QuantumGuard AI Development

Technical Skills:

Python Programming - Advanced application development with Streamlit, Pandas, NumPy

Machine Learning - Anomaly detection, clustering algorithms, predictive modelling

Database Management - PostgreSQL integration, SQLAlchemy ORM, connection pooling

Data Processing - ETL operations, data cleaning, feature extraction

API Integration - OpenAI GPT-4o implementation for natural language processing

Cryptography - Post-quantum encryption implementation and security protocols

Web Development - Interactive dashboard creation and user interface design

Analytical Skills

Financial Analysis - Transaction pattern recognition and risk assessment

Network Analysis - Graph theory application for blockchain relationships

Statistical Analysis - Outlier detection and pattern classification

Predictive Analytics - Trend forecasting and behavioural modelling

🏗️ SFIA Framework Mapping

Level 4 - Enable (Mid-Senior Level)

PROG - Programming/Software Development

- Competency: Design and develop complex software solutions
- Evidence: Built multi-component application with AI integration, database connectivity, and security features

DTAN - Data Analytics

- Competency: Perform complex data analysis and interpretation
- Evidence: Implemented advanced analytics, clustering, and predictive modelling for financial transactions

ITMG - IT Management

- Competency: Manage technical projects and system architecture
- Evidence: Designed modular architecture with security-first approach and scalable components

Level 3 - Apply (Mid Level)

DBAD - Database Administration

- Competency: Design and implement database solutions
- Evidence: PostgreSQL integration with proper connection handling and data modelling

NTAN - Network Analysis

- Competency: Analyse network patterns and relationships
- Evidence: Blockchain network analysis and transaction flow visualization

SCTY - Information Security

- Competency: Implement security measures and protocols
- Evidence: Post-quantum cryptography and secure data processing implementation

Level 2 - Assist (Junior-Mid Level)

TEST - Testing

- Competency: Execute testing procedures and quality assurance
- Evidence: Application testing, error handling, and validation implementation

VISL - Data Visualization

- Competency: Create effective data visualizations
- Evidence: Interactive charts, network graphs, and dashboard development

Competitors

DARKTRACE

USES AI TO ANALYZE NETWORK DATA, DETECT DEVIATIONS FROM TYPICAL BEHAVIOR, AND IDENTIFY THREATS IN REAL-TIME.

SENTINELONE

OFFERS AUTONOMOUS ENDPOINT PROTECTION THAT IDENTIFIES, CONTAINS, AND RESPONDS TO THREATS.

CYBEREASON

PROVIDES CYBERSECURITY ANALYTICS WITH AI-POWERED HUNTING TECHNOLOGY.

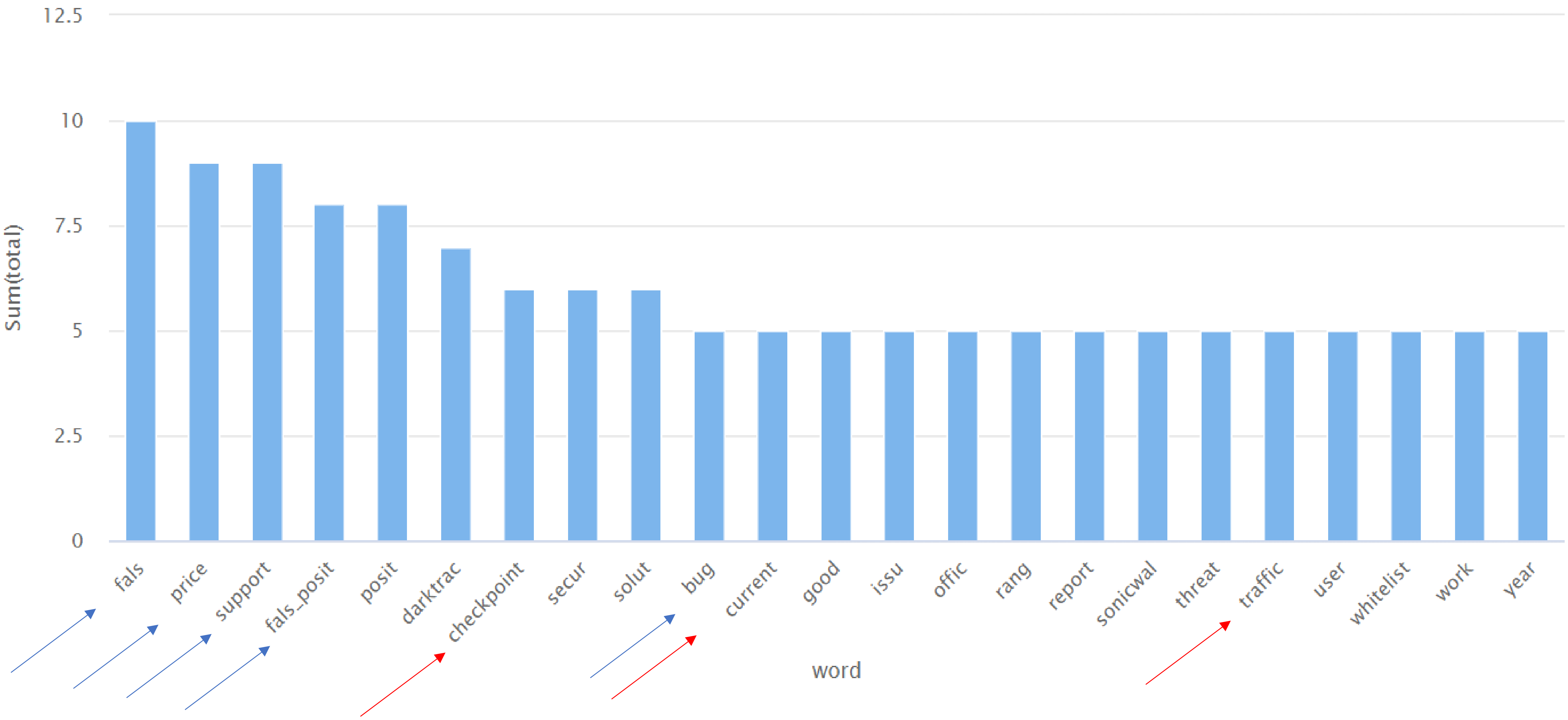
FORTINET

IMPLEMENTS AI ACROSS SECURITY PRODUCTS, INCLUDING FORTIWEB WHICH USES MACHINE LEARNING TO DETECT THREATS.

CHECK POINT

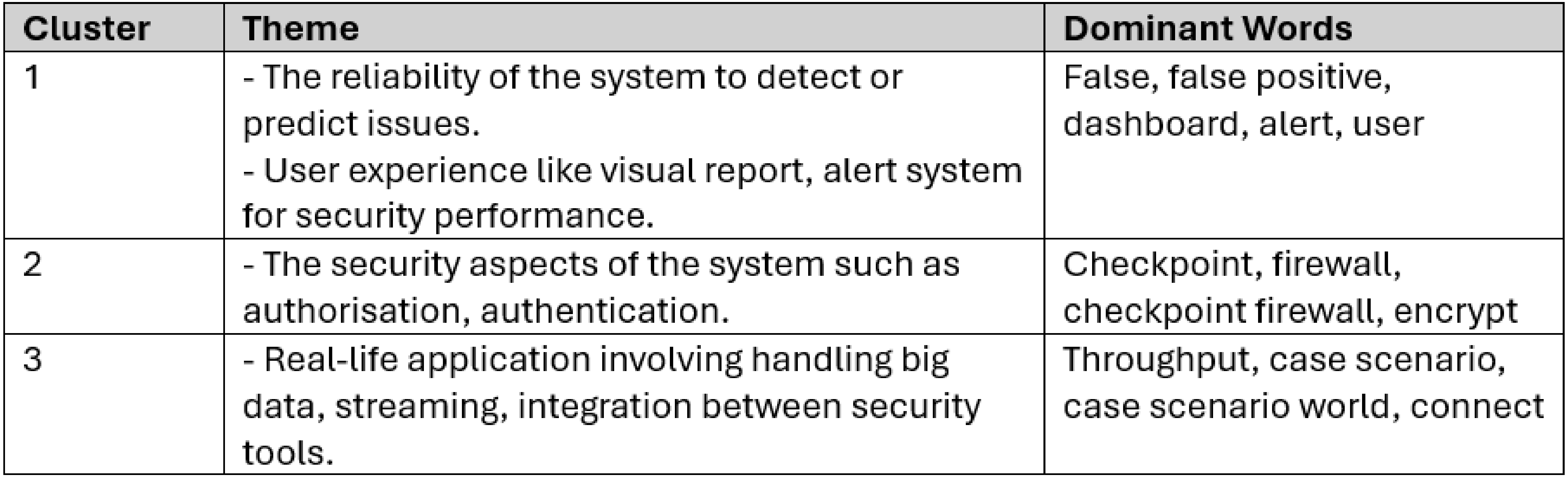
DELIVERS CUSTOMIZABLE THREAT INTELLIGENCE SOLUTIONS FOR GOVERNMENTS AND ENTERPRISES.

Top Issues In Cybersecurity Solutions



Common Themes

Involving Essential Requirements for an AI-Powered Fraud Detection System



Cluster	Theme	Dominant Words
1	- The reliability of the system to detect or predict issues. - User experience like visual report, alert system for security performance.	False, false positive, dashboard, alert, user
2	- The security aspects of the system such as authorisation, authentication.	Checkpoint, firewall, checkpoint firewall, encrypt
3	- Real-life application involving handling big data, streaming, integration between security tools.	Throughput, case scenario, case scenario world, connect

Market opportunity

1) TIMING ADVANTAGE

Growing awareness of quantum computing threats

Rising sophistication of cyber attacks

2) UNDERSERVED NICHE

Combination of quantum security, federated learning, and financial focus addresses a specific gap

Most competitors focus on either general AI security, blockchain security, or single institution solutions.

3) EXPANSION POTENTIAL

Core technology could be adapted for healthcare, government agencies, critical infrastructure

Cross-border financial transactions and settlements represent additional opportunities

Turning compliance into a selling point

•**Strong AI Governance & Ethics Compliance**: We align with ASIC’s calls for responsible AI in finance and adhere to Australia’s AI Ethics Principles set by DISR. This proactive approach supports transparency and prevents legal risks.

•**Trust Through Transparency**: Quantum Guard AI will use explainable AI to clearly show why decisions (like transaction flags) are made—addressing ASIC’s concerns about "black box" systems and promoting trust and accountability.

•**Regulatory Readiness as a Strength**: By engaging with ASIC’s Regulatory Sandbox or partnering with licensed institutions, we ensure compliance with fintech laws (e.g., data privacy, fairness). This transforms regulation into a competitive advantage, with built-in audit and AML support.

https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles

Potential of Quantum Guard AI

Commercial Potential:

- **Financial institutions** such as banks, cryptocurrency exchanges, insurance companies, can utilise Quantum Guard AI across all facets of their operations

- **Government Agency's** such as ATO, RBA and ASIC will greatly benefit in efficiently analysing finacial records, and will aid with identifying finacial and cyber crime.

- **Personal use application** can help individuals securely manage their financial accounts, make the most of tax breaks, and avoid potential legal repercussions.

Revenue Opportunities:

- The business model will likely be **SaaS (Software-as-a-Service)**. This may lead through a pilot stage, offering minimal, short-term access to organisations, to demonstrate the potential capabilities of our platform.

- Success in such a pilot could lead to a paid deployment. **Quantum Guard running in a secure Azure database, offered to clients as an API or dashboard subscription.** This allows scalability and recurring revenue.

- Additionally, positioning our product as quantum-secure analytics may attract **forward-thinking institutions**, such as AUSTRAC and ASIO, leading to potential endorsement and governemnt grants.

Overall, the commercial outlook for Quantum Guard AI is strong – financial crime compliance is a growing priority, and our solution is at the intersection of AI, blockchain, and further quantum security.

Australia has always been a late adaptor of critical advancements in technology. This works too our advantage, as we strive to pioneer AI tools into the world of Australian finacial security and growing cyber and crypto concerns.

Potential Challenges

- **Complex Implementation**

Integration of multiple advanced technologies creates technical complexity. This is even more difficult to explain to investors/Clients. Quantum-resistant cryptography implementation is still evolving, and could be obsolete by the time of implementation. The software creation and implementation process will requires extensive testing to ensure components work together seamlessly.

- **Competitive Pressure**

Several companies working in adjacent spaces and already established players have strong AI security capabilities. Some competitors even offer quantum-resistant encryption. Our potential opportunity is being one of the first to pioneer it in Australia

- **Adoption Hurdles**

Financial institutions are typically conservative with new technologies. Getting these institutions to provide their data to be analysed and trained with, requires a robust security of the database and network transfer, that is explainable to potential clientele, to build trust.

- **Resource requirements**

Significant resources such as hardware are required in computing for AI. Looking at using 3rd party software's for UI development and model training is an on-going interest. Furthermore, database infrastructure will be key for the models deep learning requirements, and ensuring its regularly updated with only relevant data for model training, will be a constantly monitored task

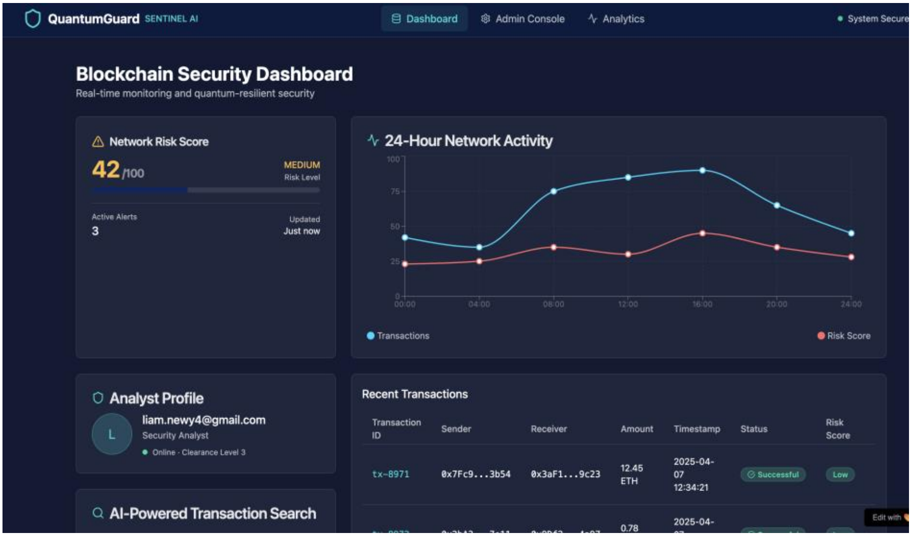
Technical Architecture

🏗️ Frontend Layer

- Streamlet Web Interface - Interactive dashboard for data upload, analysis control, and results visualization
- Multi-tab Layout - Organized sections for different analysis types and visualizations
- Real-time Updates - Dynamic content updates based on user interactions

🧠 AI & Analytics Engine

- OpenAI Integration - GPT-4o for natural language queries and intelligent insights generation
- Machine Learning Models - Scikit-learn for clustering, anomaly detection, and predictive analysis
- Advanced Analytics Module - Custom multimodal analysis combining multiple A approaches



Blockchain Security Dashboard

Real-time monitoring and quantum-resilient security

Network Risk Score

42 /100 MEDIUM Risk Level

Active Alerts 3

Updated Just now

Analyst Profile

L liam.newy4@gmail.com

Security Analyst

Online · Clearance Level 3

AI-Powered Transaction Search

Recent Transactions

Transaction ID	Sender	Receiver	Amount	Timestamp	Status	Risk Score
tx-8971	0x7Fc9...3b54	0x3aF1...9c23	12.45 ETH	2025-04-07 12:34:21	Successful	Low

🔧 Core Processing Components

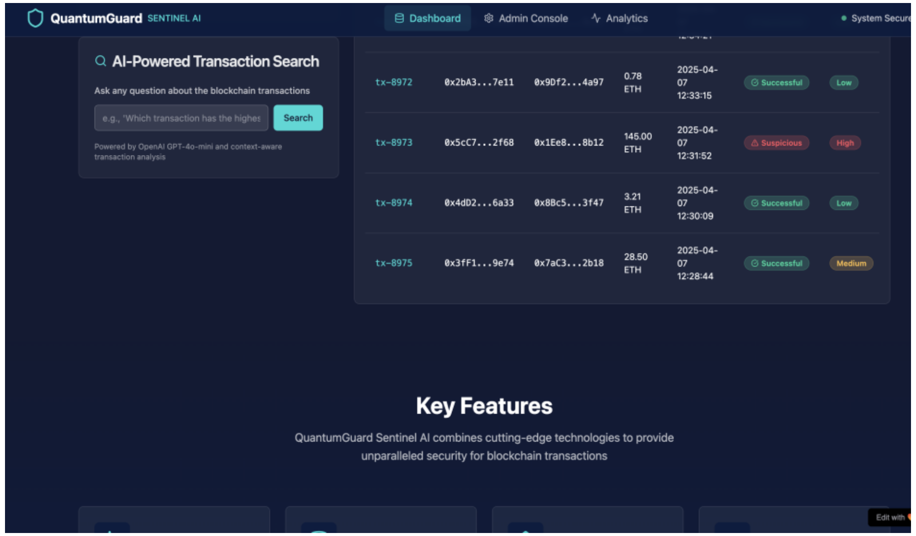
- Data Processor - Handles multiple data formats and pre-processing
- Blockchain Analyzer - Specialized logic for transaction risk assessment
- ML Models Engine - Isolation Forest, DBSCAN clustering, and custom risk scoring
- Network Analysis - Network for relationship mapping and graph metrics

🔐 Security Layer

- Post-Quantum Cryptography - Custom implementation for data encryption/decryption
- Secure Data Handling - Encrypted processing of sensitive transaction information

💾 Data Storage

- PostgreSQL Database - Persistent storage for analysis sessions and results
- SQLAlchemy ORM - Database abstraction layer with connection pooling and SSL support
- Session Management - Save/load analysis results for future reference



AI-Powered Transaction Search

Ask any question about the blockchain transactions

e.g., 'Which transaction has the highes

Powered by OpenAI GPT-4o-mini and context-aware transaction analysis

tx-8972	0x2bA3...7e11	0x9Df2...4a97	0.78 ETH	2025-04-07 12:33:15	Successful	Low
tx-8973	0x5cC7...2f68	0x1Ee8...8b12	145.00 ETH	2025-04-07 12:31:52	Suspicious	High
tx-8974	0x4dD2...6a33	0x8Bc5...3f47	3.21 ETH	2025-04-07 12:30:09	Successful	Low
tx-8975	0x3fF1...9e74	0x7aC3...2b18	28.50 ETH	2025-04-07 12:28:44	Successful	Medium

Key Features

QuantumGuard Sentinel AI combines cutting-edge technologies to provide unparalleled security for blockchain transactions

Technical architecture

Advanced Multimodal Analytics

Now combines multiple AI approaches including transaction clustering, behavioural pattern analysis, risk correlations, and network insights

- Advanced Analytics: Comprehensive multimodal analysis with clustering and pattern recognition
  Predictive Analysis: Future trend forecasting with customizable prediction horizons

🔄 Data Flow Architecture

1. Input → CSV/Excel upload or format conversion
2. Processing → Data cleaning, feature extraction, and analysis
3. Analysis → Risk assessment, anomaly detection, and AI insights
4. Storage → Database persistence with encrypted data
5. Output → Interactive visualizations and exportable reports

🚀 Scalability Features

- Modular Design - Independent components for easy maintenance and updates
- Connection Pooling - Efficient database resource management
- Retry Logic - Robust error handling for network operations

Prototype:

- https://replit.com/@liamnewy4/BlockchainSentinel
- https://lovable.dev/projects/12ce8cf2-1f0b-41eb-9776-34875c62b9e3 - 2nd version

Transaction examples:

1.Random address on etherscan

https://etherscan.io/address/0xda9dfa130df4de4673b89022ee50ff26f6ea73cf

2.The dataset contains detailed information about bank transactions for customers of LOL Bank Pvt. Ltd., with the objective of detecting fraudulent activities.

https://www.kaggle.com/datasets/marusagar/bank-transaction-fraud-detection

3.Bitcoin public csv

https://data.opendatasoft.com/explore/?flg=en-us&q=btc&sort=modified&disjunctive.language&disjunctive.source_domain_title&disjunctive.theme&disjunctive.semantic.classes&disjunctive.semantic.properties

API Key Integration

- https://platform.openai.com/api-keys

Looking forward for Quantum Guard AI

Quantum Guard AI will look to adapt to AUSTRAC’s standard. Based on deep analysis of AUSTRAC 2024-2025 priorities and Australian Big Four banks' current AI implementations,

🔥 **AUSTRAC's TOP 2024-2025 PRIORITIES:**

1. **Transaction Monitoring Programs (TMPs)** - Must identify complex, unusual patterns with broad crime type coverage
2. **Real-time suspicious activity detection** - Especially for structuring, layering, and cash-out schemes
3. **Enhanced Customer Due Diligence (ECDD)** automation
4. **Cross-sector intelligence sharing** (banks are already implementing Bio Catch Trust™ Australia)
5. **Digital currency exchange (DCE) and crypto monitoring** - Major regulatory focus
6. **Behavioural biometric intelligence** - All Big Four banks now using this

🏦 **WHAT AUSTRALIAN BANKS ARE IMPLEMENTING RIGHT NOW:**

- **CBA**: 50% reduction in scam losses using AI, analysing 20M+ payments daily
- **All Big Four**: Bio Catch behavioural biometrics pilot (October 2024)

💡 Features we are looking to add to increase competitive advantage

1. **Real-time Cross-Bank Intelligence** (BioCatch Trust™ style)
2. **Post-Quantum Cryptography Ready** (Future-proof security)
3. **AUSTRAC-Compliant by Design** (Regulatory alignment)
4. **Behavioural Biometrics Integration** (Next-gen fraud detection)
5. **Explainable AI** (SHAP integration for transparency)
6. **Generative AI Investigation Assistant** (Automated compliance)

Questions