National College of Ireland

Project Submission Sheet

Student Name: Abhijith Thanippilly Soman ………………………………………………

Student ID: X23271400 ………………………………………………

Programme: Msc Cyber Security ……………………… **Year:** 2024-2025 ………………

Module: Cryptography and Blockchain ………………………………………………

Lecturer: Vikas Sahni ………………………………………………

Submission Due Date: 17-05-2025 ………………………………………………

Project Title: TABA ………………………………………………

Word Count: 1600 ………………………………………………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Abhijith Thanippilly Soman ………………………………………………

Date: 17-05-2025 ………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Cryptography and Blockchain

TABA

Your Name/Student Number	Course	Date
Abhijith Thanippilly Soman / x23271400	Msc Cyber Security	17-05-2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

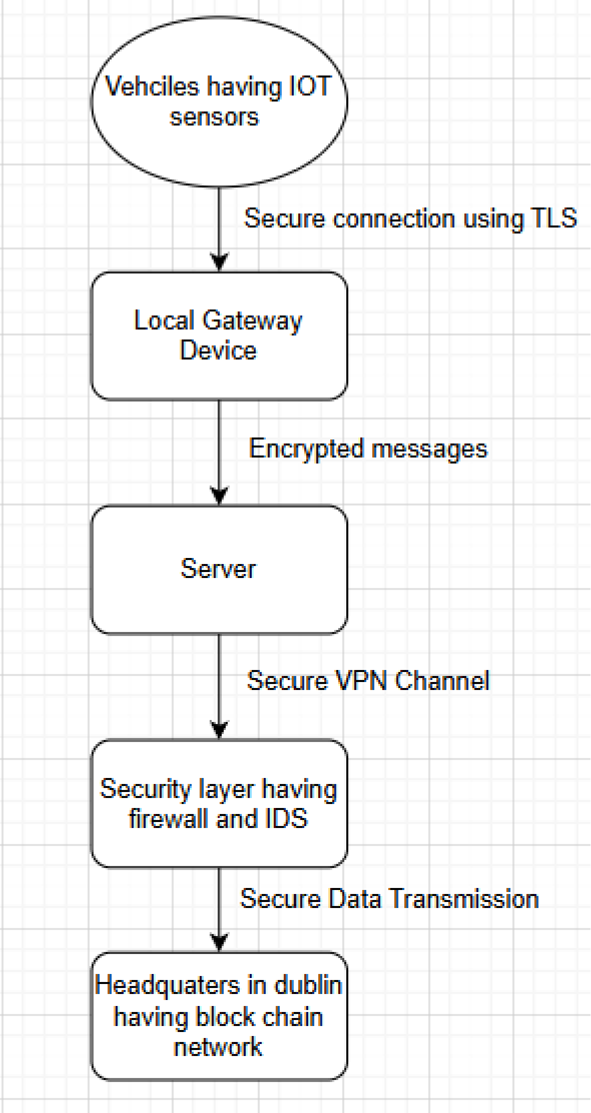
[Place evidence here]

Additional Evidence:

[Place evidence here]

1)

I) Transportation Domain – A transportation company which is headquartered in Dublin and having multiple services and transport vehicles nit across the state. It uses IOT sensors which is placed on its vehicle units, to collect and transmit sensitive data like the location, speed, environmental conditions, identity and status of driver, the goods and services being transported. These collected data from various servers is securely transited to the headquarters in Dublin through various secure layers.


Vehciles having IOT sensors
Secure connection using TLS
Local Gateway Device
Encrypted messages
Server
Secure VPN Channel
Security layer having firewall and IDS
Secure Data Transmission
Headquaters in dublin having block chain network

Components

- Vehicles having IOT sensors – they collect data from the remote vehicle like the location, cargo temperature vehicle speed etc. They collect this information and encrypt them before sending them. A secure connection is established between the target devices using technologies like TLS.
- Local Gateway device – It a device placed at some local point to collect and aggregate the information that have been transmitted by the individual sensors. This gateway performs activities like conducting a preliminary security check, configuring the encryption standards and then finally forwarding the encrypted data.
- Server – It is enforced with the duty of managing the messages and communication that is happening between the headquarters and gateways. The secure light weight messages are manged using a Message Queuing Telemetry

Transport (MQTT) broker server. It is reliable and supports real time messaging requiring very little bandwidth.

- Security layer having firewall and IDS – Ther firewall and Intrusion detection systems ensure that only legitimate traffics can pass through this security layer. The IDS can detect and alert suspicious activities while monitor the communication taking place in the network.
- Company headquarters – the headquarters in Dublin is equipped with blockchain network. This block chain network offers secure decentralised database therefore upholding features like data integrity and trust. It allows the immutability of the data as it won't be possible to ,doily the data received from the sensors. It can monito all the received data and can enforce adequate security policies and use the blockchain network to retrieve and then verify the integrity of information

II)

- Data protection – The data collect from the IOT sensors at the remote vehicle need to be securely encrypted and then transmitted. It is important to prevent interception, modification of these data. The disclosure of info like location, speed and etc can have severe bad effects on the company's operations and reputations.
  The system uses TLS encryption to communicate with local gateways. It can ensure the data confidentiality and integrity during the transmission. Transport layer security(TLS) uses advanced encryption standards like AES for data encryption and RSA cryptography for key exchanges.
  The Secure server uses MQTT over TLS and is ideal for the lightweight communications under limited bandwidth conditions. It can protect sensitive information against interception of messages and tampering of its contents.
  The secure VPN tunnels also offer a secure communication channel between the local server and the headquarters. These encrypted secure channels can provide protection against interceptions and offer confidential and integrity during the transmission.
- Block Chain network – The block chain network also provides various secure features like
  controlled access only between the authorized network – it offers security and compliance with the principles
  data Immutability- Since the data is stored using blockchain, it cannot possible to perform any modifications on them. Therefore, it can ensure the integrity the data being the received.
- Device Configuring – Each new vehicle should be attached with anew IOT deice device. This deice have a unique id and digital certificate by trusteed certification authority.
  When this IOT deice connects with local gateway server there is mutual authentication in place which validate the credentials and provides the device authenticity
  The headquarters enforces continuous security auditing and monitoring- various devices like the IDS and SIEM(Security Information and Event Management) is employed to detect anomalies int the traffic. These can easily flag the uses from the data from individual devices and can take adequate actions

2) Quantum cryptography relies on the principles on quantum mechanics while the classical cryptography relies on the mathematics.
The principles used by quantum cryptography include

- Quantum particles are naturally uncertain – they can always have different orientations and properties always
- Binary position can be used to randomly measure the quantum particles – the different polarities or spins can be used as a binary counterpart and can be represented as zeros and ones for computations and for other calculations.
- Quantum system always undergo change if it is measured: According to quantum physics, analysing or examining a quantum particle will always affect their configuration, there is no way to check a particle without any alterations happening.
- Quantum particles cannot be perfectly cloned: it is possible to partially copy the certain features of a quantum particle, it is not possible to completely make an exact copy of a quantum particle.

The quantum cryptography technique is implemented used using a method named Quantum key Distribution. This principle states that the quantum bits are sent with some random specific states like polarity. Any interception that happens on them will disturb the state, which will further alter both the sender and receiver.
For a communication of quantum particles happening between alice and bob. Alice sends quantum particles to bob in some random polarized sates. Once bob receives these particles, he starts to measure the states of the received photons. They publicly announce the bases used to set the states; the bits are discarded whose bits doesn't match. And remaining bits whose bits match are used to form a secure key.

The difference between classical cryptography include:

- The classical cryptography depended on mathematical complexity. The security for them is based on the computational difficulty of techniques used. While the quantum cryptography relies on the laws of quantum mechanics, which offers more security guarantee by the physics laws rather the computational difficulty, making the quantum cryptography more secure compared to the classical cryptography.
- Classical cryptography techniques like RSA, large number etc, can easily be broken using quantum computing techniques. But the Quantum cryptography is resilient against quantum computing attacks as it doesn't depend on the computational complexity.
- Quantum computing can easily identify a eavesdropping attempt as it will disturb the quantum states of particles, while in classical cryptography there are no ways to detect the eavesdropper.
- The classical cryptography is less expensive and widely used however its less efficient compared to the expensive and complex quantum cryptography.

3) The immutability concept is highly fundamental in Ethereum smart contracts. By this immutability concept they would be unable to undergo any further modification once they are deployed to blockchain. This property of Ethereum highly boosts the user trust, transparency of operations.

Positive aspects of immutability

- Trust - The smart contract code cannot be tampered once deployed. There is no need to enforce a centralised authority to monitor operations. It enforces a trustful environment. Users can be confident that the predefined rules will be followed, and it cannot undergo any modifications by threat actors or even by

administrative controls. Therefor it can assure that the results or final step would be based on the predefined conditions only.
- Transparency – users can easily audit how the smart contract code before interacting to know exactly how it works. Since the Ethereum is decentralized and publicly available. This feature ensures transparency and accountability ensuring all customers can clearly understand the terms of interactions.
- Decentralization: There is no need for any traditional intermediaries, which helps in reducing the cost and increasing efficiency
- Equal access: All the participants on the Ethereum network is issued with a identical ledger copy . this provides them a equal access. This equal access grants form transparency and fairness in the operations and transactions.

Negative aspects of immutability:

- Vulnerabilities in design: The immutable property ensures that once deployed no modification can be performed. This makes it difficult to patch or correct the bugs and vulnerabilities easily. As the code is immutable the developers cannot correct the issue post deployment . this can lead to significant financial losses and loss in confidence among users.
- Not flexible- The immutability prevents any changes to be adapted to comply with any unforeseen events or real-world changes. If the external conditions or government regulations change, the contract may become ineffective or non-complaint with standards. This would lead it into failure of fulfilling its intended objectives
- Loss of funds - The immutability can also lock funds permanently in a contract. These can be due any unforeseen issues or due to some issues in design or coding errors. There are numerous cases of millions in crypto have been locked in contracts leading to financial and reputational damage.

Balancing the Risks and Benefits

- Proper Audits - A proper and careful audits of smart contracts are required before deployment. It has to before carefully scrutinized and the various possibilities need to analyse. Multiple code reviews and verifications procedures should be performed to identify the potential vulnerabilities before deploying the contracts.
- Upgradable contracts – Proxy contracts having some limited upgradability can be deployed. The main contact can forward calls to this new contract which has fix or modifications to the existing flaw logic. This can ensure adjustments and can reduce negative consequences.
- Community governance – in cases extreme requirements communities can implement hard forks although it can introduce controversies and hinder the basic immutability logic. But it can be used as final measure to solve the critical issues.

The feature that the Ethereum smart contracts cannot be altered offers transparency, trust and decentralized security. On the other hand, it possesses some significant limitations, like it can be affected by small errors and cannot not easily adjust to new changes. But to strike a balance, the community needs to ensure that Ethereum remains resilient with some changes, always ensuring safety, trust and the adherence of its principles.