



QUEENSLAND UNIVERSITY
OF TECHNOLOGY

IFN711 PROJECT FINAL REPORT

The reliable spark plugs

TEAM 5

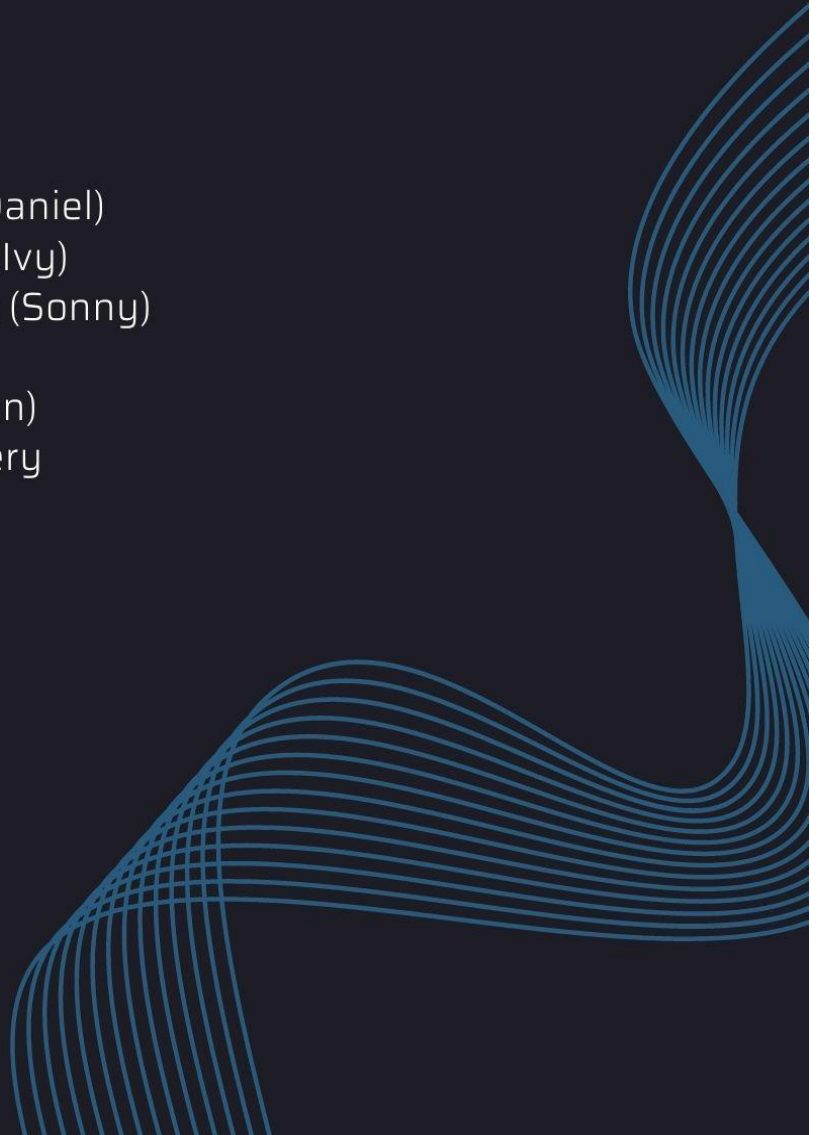
N9926593 Dong Xi Cai (Daniel)
N9930001 Xu Tong Wan (Ivy)
N10313907 Yu Xuan Shen (Sonny)
N9645951 Lin Chen
N9845712 Yi Jun Xu (Vivian)
N9334963 Bader Alkandery

TUTOR

Dr Bhargavi Goswami

INDUSTRY PARTNERS

Dr Shantanu Pal
Dr Zahra Jadidi



IFN711 | Industry Project Assessment 2 | Rubric: Final Project Report & IT Artefacts

Criteria	High Distinction	Distinction	Credit	Pass	Fail
Project Outcome and success <ul style="list-style-type: none"> Value Useful Complete 	Demonstrates a sophisticated understanding of the project context including the nature of the business or organization and the sector within which it operates	Demonstrates a high understanding of the project context including the nature of the business or organization and the sector within which it operates	Demonstrates a good understanding of the project context including the nature of the business or organization and the sector within which it operates	Demonstrates an understanding of some significant aspects of the project including the nature of the business or industry.	Does not display an understanding of the project correctly, significant aspects missing.
25 marks	The project goals are listed and explained so that their impact is clear. There is a clear and professional assessment of the extent to which the goals were achieved, and explanation provided as to how the assessment was achieved including any metrics use for evaluation.	The project goals are listed and explained clearly but lack sophisticated engagement and depth of understanding. An evaluation of effectiveness is clearly presented but lacking depth of engagement and inclusion of logical rationale or metric.	Project goals are listed and an explanation is provided but is missing clear articulation of their impact and value. A general assessment of success is included with limited depth and no inclusion of rationale or evaluative metric.	The project goals are presented but not explained with depth or detail. Most information is pertinent to the project. A simplistic assessment of success is included with limited, or no rationale or evaluative metric included.	Reasoning is deficient. Information is not relevant or flawed. Project goals are not articulated, incorrect or unprofessional in engagement
Project Progress & Reflections <ul style="list-style-type: none"> Critical Analysis Problem Solving Efficiencies Effectiveness 	<ul style="list-style-type: none"> The project increments were executed completely as outlined in the Assessment 2 Project Plan All increment level evidence on the project progress is included using accepted tools (Trello images, burndown charts, Gantt Charts and retrospective records) Revisions to the Assessment 2 Project Plan are discussed and justified professionally. Relevant experiences related to issues your group faced are critically analysed, presented with insightful resolutions 	<ul style="list-style-type: none"> The project increments were executed mostly as outlined in the Assessment 2 Project Plan Most increment level evidence on the project progress is included using accepted tools (Trello images, burndown charts, Gantt Charts and retrospective records) Revisions to the Assessment 2 Project Plan are discussed in detail and justified Relevant experiences related to group level issues are properly analysed, presented with original resolutions 	<ul style="list-style-type: none"> The project increments were executed partly as outlined in the Assessment 2 Project Plan Some of the increment level evidence on the project progress is included using accepted tools (Trello images, burndown charts, Gantt Charts and retrospective records) Revisions to the Assessment 2 Project Plan are described with limited justifications Relevant experiences related to group level issues are analysed, presented with basic resolutions 	<ul style="list-style-type: none"> Most of the project increments did not deliver meaningful outcomes The increment level evidence on the project progress is not relevant or not included from the tools (Trello images, burndown charts, Gantt Charts and retrospective records, "Done" lists) Limited Revisions to the Assessment 2 Project Plan are mentioned Relevant experiences related to group level issues are not discussed 	<ul style="list-style-type: none"> No useful outcomes were delivered in all increments The increment level evidence on the project progress is not included from accepted tools (Trello images, burndown charts, Gantt Charts and retrospective records) Revisions to the Assessment 2 Project Plan are not covered at all Relevant experiences related to group level issues are not discussed (no group level reflections)
IT artefacts Delivered to the customer <ul style="list-style-type: none"> Quality Professional Standards 	<p>The artefacts and its subcomponents submission fully match with the scope agreed with the client</p> <p>Those are delivered to with high quality standards and well above normal expectations of the industry partner or tutor</p> <p>The IT artefacts are indistinguishable from one produced in a similar time frame by an experienced professional team.</p>	<p>The artefact submission encompasses much of the scope agreed with the client or tutor but falls short in several important areas, with key components either not attempted or completed, or completed well below a professional standard.</p> <p>Overall, the artefact reflects work of a good standard for the work successfully delivered, while remaining below the level as those in the higher-grade band.</p>	<p>The artefact submission broadly reflects the scope agreed with the client, but some aspects of the agreed deliverable may not have been completed or may not have been completed to a professional standard.</p> <p>Overall, the artefact reflects work of a near professional standard for the work successfully delivered, without perhaps reaching the same level as those in the higher-grade band.</p>	<p>The artefact submission encompasses some of the scope agreed with the client but falls well short of an acceptable deliverable for the project.</p> <p>Key components are either not attempted or completed poorly.</p> <p>Overall, the artefact reflects work of a relatively weak standard for the work successfully delivered,</p>	<p>The artefact submission encompasses little or none of the scope agreed with the client or tutor</p> <p>None of the agreed components of the artefact have been delivered, and those mentioned are of poor quality.</p> <p>Key components are either not attempted or</p>
40 marks					

The work generally reflects a standard at normal expectations of a team of Master of IT final year students.

completed or completed poorly.

<p>Communications</p> <ul style="list-style-type: none"> • <i>Clarity</i> • <i>Conciseness</i> • <i>Correctness</i> <p>10 marks</p>	<p>The report is consistently professional in tone and structure and addresses each of the listed requirements in great detail</p> <p>No errors of grammar or structure.</p> <p>Report is organized to aid understanding, and this is assisted by the layout and formatting.</p> <p>The standard of writing exceeds well above expectations</p>	<p>The report is generally professional in tone and structure and addresses each of the listed requirements in detail</p> <p>Very limited errors in grammar or structure.</p> <p>The report is well organized, and the layout and formatting are well chosen.</p> <p>The standard of writing is above expectations</p>	<p>The report is professional in tone and structure but lacks some detail in a small number of the listed requirements.</p> <p>There may be frequent and occasional errors of grammar or structure.</p> <p>Organization and layout remain good,</p> <p>The standard of writing meets the expectations of this level.</p>	<p>The report does not meet expectations, and the coverage is deficient in several the listed requirements.</p> <p>Grammar and structure are variable but are usually ok.</p> <p>The organization is deficient, but some effort has been made to structure and format the document.</p> <p>The standard of writing may lie below the expectations at this level</p>	<p>The report doesn't meet the requirements set out in the brief.</p> <p>Sections missing or poorly covered.</p> <p>Meaning unclear as grammar and/or spelling contain frequent errors</p> <p>Disorganised or incoherent writing</p> <p>Structure either absent or incoherent and the standard of writing may be well below the expectations at this level</p>
--	---	--	--	---	--

Executive Summary.

In recent years, with the development of science and technology, more and more organizations rely on Information Technology (IT), in which maintaining the network security of the organization becomes crucial. In response to increasingly sophisticated means of countering attackers, the technology of cyber threats intelligence (CTI) has been proposed. Based on Dalziel(2015), cyber threat intelligence is data collected, processed, and analyzed to understand the motivations, targeting, and attack behaviour of threat actors. Threat intelligence enables us to make faster, smarter, data-backed security decisions and change the behaviour of threat actors from reactive to proactive when confronting them. According to Moore(2021), the importance of CTI is mentioned: In the cybersecurity world, Advanced Persistent Threats (APTs) and defenders are constantly trying to outsmart them (Baker, 2022). Data on the next steps of threat actors is critical to proactively tailor defences and preempt future attacks. In continuous development, only collecting intelligence is not enough. So considering how to share intelligence efficiently. Blockchain is a very fast, safe and convenient platform for information sharing. In this project, our team will submit two artefacts, one of them is to develop a website app that can be used for CTI sharing using the blockchain-based hyper ledger platform. The second is a literature review in the fields of CTI and blockchain. This report will consist of four parts: project analyses, artefact design, outcome and group reflection.

Table of Contents

Executive Summary.	3
1 Analysis.	5
1.1 Project overview.	5
1.1.1 Problem scope	5
1.1.2 Literature review	5
1.2 Acceptance Criteria	7
1.3 Project process management	7
2 Design.	9
2.1 UI design	9
2.1.1 Initial prototyping configuration	9
2.1.2 Homepage:	9
2.1.3 Website Design Concept:	9
2.1.4 Honeycomb framework	9
2.2 Front-end design	10
2.2.1 Front-end overview	10
2.3 Back-end design	10
2.3.1 Fabric network	10
2.3.2 compilation process	11
2.4 Interaction	11
3 Outcomes.	13
3.1 Main Result.	13
3.2 Improvement and future directions	13
3.3 Test Activity	15
3.4 Evaluation Indicators	19
4 Group Reflection.	22
5 Reference.	24
6 Appendix.	25
6.1 Team Performance Control	25
6.2 Functional and nonfunctional requirements	27
6.3 Risk management	30
6.4 Burndown chart.	31

1 Analysis.

1.1 Project overview.

1.1.1 Problem scope

In this project, We analyse the key issues in the research area. The first one CTI and blockchain combined is the Lack of in-depth research. Many technologies are immature and still in the theoretical and prototype stage. There are also few papers and reference materials in the professional field, and everyone is just starting in this field. There are many centralized CTI sharing platforms now. However, the centrally managed CTI platform has many drawbacks. The first is that the speed of publishing information and others receiving information is relatively slow. Secondly, if the platform is attacked, it will cause many problems. Therefore, compared with the traditional CTI platform, it is a better choice to release CTI through a decentralized Blockchain. But the third problem also arises: Anyone can publish information on Blockchain, which will lead to complicated information. Therefore, the blockchain platform Hyperledger, which combines permission design, has become a very outstanding platform. This project is also developed around the fabric in Hyperledger. The following will introduce the development ideas and results in detail.

1.1.2 Literature review

The first stage: search in academic databases

To achieve the research objectives, search accessible databases such as Springer Link, Web of Science, and Scopus to identify published research papers. All results are limited to the English language and the publication year is between 2010-2021. Our research revealed the following time span for analytical research articles: 2010 to 2021. The reason for these limitations is that Blockchain is an emerging technology that is developing very fast and the number of research articles has increased significantly. It should be kept in mind that there may be differences between the early application of Blockchain in education and the new research in recent times. Therefore, I set the target for publications after 2010. The initial search was based on keywords, namely "blockchain" and "Cyber threat intelligence". We searched a total of 2,068 documents, including articles, reviews, books, book chapters, editorials, and conference papers. The number of documents containing the above keywords was recorded. We have analyzed types of academic search engines and databases.

1) In such databases as Web of Science, Scopus, and SpringerLink, we have found 2,068 sources by applying the phrase "Sharing Cyber threat intelligence by blockchain" from 2010 to 2021. "Fig.1" presents their content type distribution.

Content Type	
Chapter	894
Book	881
Conference Proceedings	467
Conference Paper	285
Article	258
Reference Work Entry	35
Reference Work	20

2) Most of the articles dealing with blockchain applications are related to seven scientific fields: Computer Science, Engineering, Business and Management, Finance, Economics, Education, and Environment. "Fig.2" presents Involved field classification.

Discipline	see all
Computer Science	720
Engineering	626
Business and Management	279
Finance	99
Economics	72

The second stage: visual observation

Next, according to the keyword search, there are many articles unrelated to the topic. First, we excluded articles that were not relevant to the topic. Then we decided to narrow it down further. To make reading easier, we will use English articles as search criteria. Furthermore, to make the results more meaningful, we included criteria that excluded conference proceedings, conference papers, and editorials. The included literature should be related to blockchain, CTI sharing, and Hyperledger Fabric. Based on the above criteria, we finally selected 50 journals or books from 2068 articles from 2010 to 2021 that met the inclusion criteria. In my opinion, the more citations it gets, the more people know about the article. Therefore, after this stage, we use Publish or Perish (a citation analysis and literature search application) to select the 20 most cited articles.

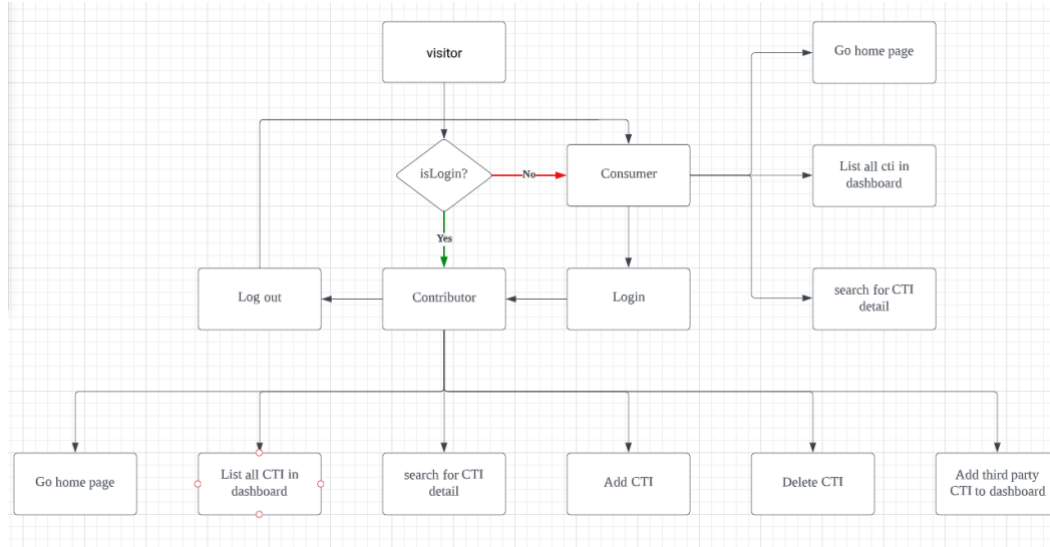
The third stage: Collection

Except for these 20 articles, we also added 30 articles searched from Google scholar, QUT library and other sources to our literature list.

Throughout the semester our group was collecting and summarised articles to be used for the literature review. Our academic partners Dr.Pal and Dr.Jadidi requested a literature review to be one of the project deliverables, and mainly to focus on the future challenges of sharing CTIs over a blockchain. We have read many articles which stand out in our literature review. The literature review would be helpful to our academic partners by saving their valuable time finding resources. In short, our literature review presents the analysis of various literature on sharing cyber threat intelligence using blockchain, giving a closer look at the future challenges of sharing cyber threat intelligence using blockchain.

1.2 Acceptance Criteria.

The requirements list shown in Appendix 6.2, contains functional requirements and non-functional requirements. According to the requirements we design the flow chart down below:



We need to use the blockchain to share CTI, in which the consumer needs to obtain the CTI information in our app for subsequent operations such as use or analysis. As the provider of CTI, Contributor intends to use two methods: 1. Input the CTI information to be added to the ledger through a fixed format. 2. Add the CTI information obtained by the third party to the ledger.

Therefore, we need to use the blockchain to provide a ledger that all users can view and search for common CTI information. This function can be achieved by using the channel in Fabric. In addition, we also need to provide Chaincode to perform operations such as adding, deleting, modifying, and checking the CTI information in the ledger to improve the characteristics of the blockchain. We will use the query and invoke functions in Chaincode to achieve this. Third, the functions in Chaincode can only be called in the peer node environment, which is very inconvenient, we will provide an app with node.js as the framework to call Chaincode. So the node command can operate on the ledger. Because our website development strategy requires a separate front-end and back-end design, we provide an API port developed with node.js express for front-end access. The front-end calls the function of the back-end through the API to update the ledger, and the returned data format is JSON, which is convenient for front-end rendering.

1.3 Project process management

In this project, we used DSDM (Dynamic System Development Method) to manage the life cycle of the project. The DSDM model prioritizes the business case, ensuring that any project delivered by the team has critical business value. It provides basic product functionality quickly. Developers can easily access their end-users. Projects are easier to stay within budget (WAEL&SUFYAN,2019). Based on DSDM, we have formulated a grouping plan for the group: the group of 6 people will be divided into a front-end development group and a back-end development group to write code simultaneously, and all members will collect literature review materials, and two people

will be responsible for writing. At the same time, we assign each member a specific position based on the member's ability and professionalism. As shown below.

Member	Special Role	Common Role			
		Front-end team	Back-end team	Literature Review	Literature Collection
Yuxuan Shen(Sonny)	Main software developer	✓	✓		✓
Yijun Xu(Vivian)	Leader/Process manager		✓		✓
Bader Alkandery(Bader)	Scrum master		✓	✓	✓
Dongxi Cai(Daniel)	Front-end developer	✓			✓
Xutong Wan(Ivy)	Front-end developer	✓			✓
Lin Chen(Lin)	UI/UX designer	✓		✓	✓

We also conducted risk assessments, and process assessments, and developed group protocols. We also made a requirement list (All in the Appendix) based on MoSCow's prioritization. The development process went according to plan, and the members were very cooperative. The results were also satisfactory.

2 Design.

2.1 UI design

2.1.1 Initial prototyping configuration

The simple configuration of the front end is before the development of the back end. The website is mainly divided into 4 functions on the navigation bar. For example, users can register new accounts and log in to existing accounts. Function buttons for editing personal information and searching CTI.

2.1.2 Homepage:

The homepage is the platform to access the entire website. This page displays the introduction and important information about the website. The navigation bar at the top of the home page showcases the functionality of the site, including search, login and registration.

2.1.3 Website Design Concept:

The iceberg is used as the background for the website. The massive internet database is like an iceberg. The part above the water surface is just the tip of the iceberg, more and deeper data is underwater. On this site, users can search not only for specific CTI data. In addition, contributors can also add and delete data. In today's internet world, what users have access to is only the tip of the iceberg. So, if 5% of the internet world is visible, close to 95%+ of the data flow is in the invisible darknet flow.

2.1.4 Honeycomb framework

The honeycomb framework was developed by Peter Morville (Morville, 2004)

- Useful: The site provides users and searches for CTI.
- Usable: Information is accurate and searchable, and users can view detailed information on all CTIs. Users (contributors) can also add and delete CTI data.
- Findable: Information needs to be findable and easy to navigate.
- Credible: The website has secure access and other security features, such as the need for users to register for an account.
- Accessible: The site enables users with disabilities to have the same user experience as everyone else.
- Desirable: The interface is directly accessible for easy searching.
- Valuable: This website feature can reduce support centre costs and increase customer satisfaction.

2.2 Front-end design

2.2.1 Front-end overview

- Login:

Since the information within our ledger is transparent, and with all the security issues surrounding CTI, our initial focus for the design was to create a permission ability, intending to separate our consumer and contributor users. Due to an issue with our time, we did not utilize a database, instead, we used cookies from reacting, to add a state in our browser in our case the login function. Cookies are small files that are stored on a user's computer. It is designed to hold some site's user data so that the server can customize content for such users. The page code can get the cookie value and send it to the server.

- CTI dashboard(show all CTI):

Show All CTI page listed the detail of CTI(ID, Timestamp, Type, From) by clicking the button(Show all CTI in the ledger). The implementation of this function is that utilised the ACIOS with gateway request the API interface of the back-end GetAllCTI function.

- Search CTI

Exploiting the Search button to discover the detail of CTI depends on the ID of CTI. The use of ACIOS is adding CTI ID into URL as character splicing, and through the gateway to request the API interface of ReadCTI function in the back-end.

- Add CTI

Add CTI only can be executed by contributor, the above information needs to be filled correctly when the user click adds button. The accomplish step for this function is also exploiting the ACIO to fill in the CTI ID, LOC, Target, Timestamp, Type and From as character splicing into URL, through the gateway to request the API interface of the AddCTI function in the back-end.

- Delete CTI

The step of Delete CTI needs to fill in the CTI's ID by the contributor to click the delete button. Using ACIO to fill in the CTI ID, LOC, Target, Timestamp, Type and From as character splicing into URL, through the gateway to request the API interface of DeleteCTI function in the back-end.

- Third-Party CTI

Utilised the Click to add CTIs from CIRCL to the ledger to add third-party CTI. The principle for achieving Third-Party CTI is to use the CTI information of CIRCL with the local JSON file format.

2.3 Back-end design

2.3.1 Fabric network

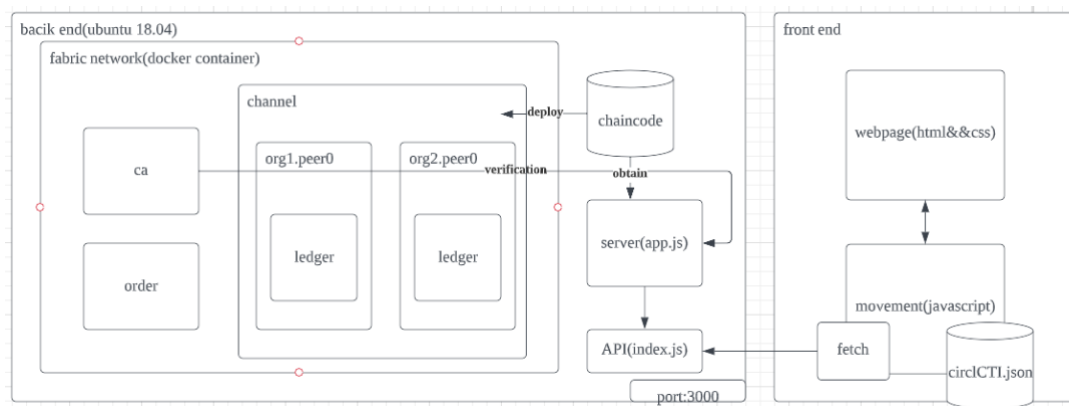
The artefact is developed using Hyperledger Fabric. Hyperledger Fabric is used as a foundation for developing applications or solutions with a modular architecture. It allows components. Its modular and versatile design meets a wide range of industry use cases. It enables large-scale performance while preserving privacy. At the same time, the finished product uses docker technology. Docker is a

technology that allows the software to be packaged and run in isolated containers. Fabric components can be run as binaries or as Docker containers. Fabric provides Docker images for all its components. The CouchDB used by Hyperledger also comes with its own Docker image. In the process of software development, we used the ubuntu18.04 version of the WSL2 virtual machine as the development environment. WSL2's architecture powers the Windows Subsystem for Linux to run ELF64 Linux binaries on Windows.

2.3.2 compilation process

When compiling the code, the team used the test network that comes with the fabric. During the development process, because our purpose is not to formally deploy but to build a prototype, we don't need a lot of peers. And then, the team add all peers of two organizations to the channel. The next step is to deploy Chaincode to the joined channel. In Hyperledger Fabric, Chaincode is "smart contracts" that run on peer nodes and create transactions. It enables users to create transactions and update the world state of assets in the shared ledger of the Hyperledger Fabric network. Applications interact with the blockchain ledger through Chaincode. Therefore, the Chaincode needs to be installed on every peer that will endorse the transaction and instantiate it on the channel. We reference two functions from chain code: Query and Invoke. Query does not generate a new block. It just returns the stored data to the front end. We added two functions: view all CTIs and find CTIs, namely showAllCTI() and readCTI(). Invoke generates new blocks, and the function needs to be called, we added three functions: delete existing CTI, add new CTI and replace CTI. They are: deleteCTI(), updateCTI() and addCTI().

2.4 Interaction



The diagram above illustrates how the back and front ends of our interface interact with each other. Within our front-end interface, it is illustrated using HTML and styled using CSS. To allow our users to interact with our front-end application, we use javascript to illustrate our movement.

We used an API management tool node.js express as a tool that sits between our front end and back end, as a reverse proxy that accepts all application programming interface (API) calls and returns the desired result. We were able to solve our cross-domain problems using proxy given that both our front and backend are run based on the same local host. we use Axios for our backend app, which will combine the

parameter and send it to our backend interface, which allows our backend app to transit into chain code, invoked by our backend app and return the search result.

3 Outcomes.

3.1 Main Result.

After a semester of research, development and design by the team, our target project (CTI sharing) has finally been completed. The goal of our project is to achieve efficient sharing of CTI data through Hyperledger Blockchain. Our platform now implements a complete, reliable, ready-to-use web app. The main functions of artifacts are listed below.

1. A complete user rights distribution system. The system provides different functions to users with different permissions by checking whether the user has logged in. The consumer can only view and find information, and the contributor can add, delete and modify information. This ensures that the consumer and contributor have different permissions.
2. Perfect CTI display panel system. The system lists the CTI IDs, timestamps, etc. of all CTIs in the backend blockchain ledger.
3. Perfect search system. The system supports users to directly input the CTI ID of the detail they want to view through the search box, and the system will match the CTI information in the ledger according to the ID entered by the user and display it in the card below the input box.
4. Perfect add function. This function only allows the contributor to input the fixed-format information of the CTI. After clicking the button, the CTI will be added to the blockchain ledger and a new block will be generated
5. Perfect delete function. The system only allows the contributor to input the ID of the CTI to be deleted, and the system will delete the matching CTI information based on the ID. When the ID does not exist, a prompt message will be returned.
6. Perfect CTI update function. This function only allows the contributor to input the information of the CTI to be updated. The system will match the ID of the CTI. If it does not exist, it will return the prompt information. If it exists, the updated CTI information will be recorded in the ledger, and the blockchain will generate new blocks.
7. A relatively complete third-party CTI addition function. This function only supports the contributor to add CTI data from third parties to the blockchain, and the added CTI will be displayed in the dashboard.

3.2 Improvement and future directions

1. Due to lack of time, the backend of the project is built in the local wsl2 ubuntu, and the availability is very low. In the future, the nodes of the backend blockchain can be deployed in the AWS virtual machine, which is convenient for maintenance and long-term use.
2. The third-party CTI in this project uses the local file in JSON format downloaded by CIRCL, which was originally intended to be obtained by API, but no suitable free resources were found. In addition, the third-party CTI

function is extensible, and multiple sources can be added in the future, just use Axios/fetch to obtain data from other APIs.

3. This project only provides two nodes as an experiment, and a multi-node fabric network can be manually constructed in the future. At first, it was envisaged that the permissions of consumers and contributors should be divided by the organization in the fabric network, but because the time is too tight, Hyperledger is new knowledge and the proficiency is not high. Therefore, we can only use cookies on the front-end to make a simple division of the login system.

3.3 Test Activity

The following shows the team's testing activities for the reliability of all verification results based on the completion of all functions of the platform. and a framework of evaluation metrics for all testing activities.

	Test list	Test detail	Result
Front end	Register	Register a new account	fail
	Login	Input the user information	success
		Press confirm button and check if the page jump	success
		The value of Cookie isLogin and check if changed	success
	Add CTI	Input the information of CTI	success
		Press confirm button and check if the page jump	success
		If the new information is displayed in the CTI dashboard	success
		If the new blockchain ledger create	success
	Delete CTI	Search the existing ID of current CTI	success
		Press confirm button and check if the page jump	success
		If the CTI disappear in the CTI dashboard	success
		If the new blockchain ledger create	success
	Show all CTI	If click the button to display all the added information	success
		Press next page button and check if the page jump	success
		Press last page button and check if the	success

		<i>page jump</i>	
		<i>Click the certain information to check the details</i>	<i>success</i>
	<i>Search CTI</i>	<i>Input the CTI ID</i>	<i>success</i>
		<i>Press check button and check if the page jump</i>	<i>success</i>
		<i>Check if the correct CTI displayed</i>	<i>success</i>
	<i>Update CTI</i>	<i>Input the CTI information</i>	<i>success</i>
		<i>Check if the CTI ID is existing</i>	<i>success</i>
		<i>Replace the new information with current inputs down the existing CTI ID</i>	<i>success</i>
		<i>Display the new details in the CTI dashboard</i>	<i>success</i>
		<i>If the new blockchain ledger create</i>	<i>success</i>
	<i>Return to homepage</i>	<i>Press the return button check if the page jump</i>	<i>success</i>
		<i>If homepage display</i>	<i>success</i>
	<i>Third Party</i>	<i>Add Third party resources with API</i>	<i>fail</i>
		<i>Press the button check if JSON API add to blockchain ledger</i>	<i>success</i>
		<i>If display the new CTI in the CTI dashboard</i>	<i>success</i>
		<i>If the new blockchain ledger create</i>	<i>success</i>
<i>Back end</i>	<i>Create Fabric network</i>	<i>Start the CA container</i>	<i>success</i>
		<i>Start the Org1.peer0 container</i>	<i>success</i>

		Start the Org2.peer0 container		success
		Start the Orderer container		success
	Add node to channel	Add Org1.peer0 to 'mychannel'		success
		Add Org2.peer0 to 'mychannel'		success
	chaincode	query	Query to show all CTI	success
			Return error message if failed	success
			Query to a CTI data by ID	success
			Return error message if failed	success
		invoke	Add CTI and generate new block	success
			Return error message if failed	success
			Delete CTI and generate new block	success
			Return error message if failed	success
			Update CTI and generate new block	success
			Return error message if failed	success
		Deploy Chaincode to 'mychannel'		success
	Backend application	Control chaincode function showAllCTI() and return result		success
		Return error message if failed		success
		Control chaincode function ReadCTI () and return result		success
		Return error message if failed		success
		Control chaincode function CreateCTI ()		success

		<i>and return result</i>	
		<i>Return error message if failed</i>	<i>success</i>
		<i>Control chaincode function UpdateCTI () and return result</i>	<i>success</i>
		<i>Return error message if failed</i>	<i>success</i>
		<i>Control chaincode function DeleteCTI () and return result</i>	<i>success</i>
<i>connectivity</i>	<i>Api gateway</i>	<i>Query '/api/read'</i>	<i>success</i>
		<i>Return error message if failed</i>	<i>success</i>
		<i>Query '/api/get-all'</i>	<i>success</i>
		<i>Return error message if failed</i>	<i>success</i>
		<i>Query '/api/delete'</i>	<i>success</i>
		<i>Return error message if failed</i>	<i>success</i>
		<i>Query '/api/update'</i>	<i>success</i>
		<i>Return error message if failed</i>	<i>success</i>
		<i>Query '/api/create'</i>	<i>success</i>

3.4 Evaluation Indicators

	experience guidelines			
Login	<ul style="list-style-type: none"> - Contributor can log in normally - User permissions change after login - Use a database to store contributor accounts - There is a message showing the status logged in - Click on the page that requires contributor permissions can automatically 	<ul style="list-style-type: none"> - Contributor can log in normally - User permissions change after login - How cookies are used to store browser state - There is a message showing the status logged in - Clicking on a page that requires contributor permissions cannot automatically jump to the 	<ul style="list-style-type: none"> - Contributor can log in normally - User permissions have not changed after login - There is a message showing the status logged in - Clicking on the login page does not jump 	<ul style="list-style-type: none"> - Can't log in normally
	<ul style="list-style-type: none"> - jump to the login page - The page jumps successfully 	<ul style="list-style-type: none"> - login page - Click to log in may jump to other pages 		
Log out	<ul style="list-style-type: none"> - can log out normally - Jump to the login page - User permissions changed from contributor to consumer 	<ul style="list-style-type: none"> - can log out normally - User permissions changed from contributor to consumer - page jump problem 	<ul style="list-style-type: none"> - can log out normally - Problem with changing user permissions - The page does not jump 	<ul style="list-style-type: none"> - cannot log out
Add CTI	<ul style="list-style-type: none"> - The page is displayed normally - Display the added CTI in the dashboard after the button is clicked - Generate new blocks and 	<ul style="list-style-type: none"> - The page is displayed normally - Display the added CTI in the dashboard after the button is clicked - Generate new blocks and 	<ul style="list-style-type: none"> - The page is displayed normally - Display the added CTI in the dashboard after the button is clicked - Generate new blocks and 	<ul style="list-style-type: none"> - function not implemented - The added CTI cannot be displayed in the dashboard after the button is clicked - Cannot generate new

	<i>hashes</i> <ul style="list-style-type: none"> - Success: The message that has been added successfully appears - Failed: A message that failed to add appeared 	<i>hashes</i> <ul style="list-style-type: none"> - no message 	<i>hashes</i>	<i>blocks and hashes</i>
Delete CTI	<ul style="list-style-type: none"> - The page is displayed normally - Delete the CTI in the dashboard after the button is clicked - Generate new blocks and hashes - Success: a message with a successful 	<ul style="list-style-type: none"> - Failed: A message indicating that the deletion failed - Delete the CTI in the dashboard after the button is clicked - Generate new blocks and hashes - no message 	<ul style="list-style-type: none"> - The page is displayed normally - Delete the CTI in the dashboard after the button is clicked - Generate new blocks and hashes 	<ul style="list-style-type: none"> - function not implemented - The CTI cannot be deleted in the dashboard after the button is clicked - Cannot generate new blocks and hashes
	<i>deletion appears</i> <ul style="list-style-type: none"> - Failed: A message indicating that the deletion failed 	<i>shows</i>		
CTI dashboard	<ul style="list-style-type: none"> - The page is displayed normally - Display all CTI information in the dashboard smoothly after clicking the button 	<ul style="list-style-type: none"> - The page is displayed normally - Show all CTI info in dashboard after button click but not smoothly 	<ul style="list-style-type: none"> - The page is displayed normally - After clicking the button, only part of the CTI information can be displayed in the dashboard 	<ul style="list-style-type: none"> - function not implemented
Search CTI	<ul style="list-style-type: none"> - The page is displayed normally - After entering the ID, click the button to display the CTI 	<ul style="list-style-type: none"> - The page is displayed normally - After entering the ID, click the button to display the CTI 	<ul style="list-style-type: none"> - The page is displayed normally - After clicking the button, only part of the CTI 	<ul style="list-style-type: none"> - function not implemented

	<i>details smoothly</i>	<i>details but not smoothly</i>	<i>information can be displayed</i>	
<i>Update CTI</i>	<ul style="list-style-type: none"> - The page is displayed normally - The CTI information is updated in the dashboard after the button is clicked - Generate new blocks and hashes - Success: a message with a successful addition appears - Failed: A message indicating that the addition failed 	<ul style="list-style-type: none"> - The page is displayed normally - The CTI information is updated in the dashboard after the button is clicked - Generate new blocks and hashes - no message display - Process smoothly 	<ul style="list-style-type: none"> - The page is displayed normally - The CTI information is updated in the dashboard after the button is clicked - Generate new blocks and hashes - Process not smoothly 	<ul style="list-style-type: none"> - function not implemented - The CTI cannot be updated in the dashboard after the button is clicked - Cannot generate new blocks and hashes

<i>Third Party</i>	<ul style="list-style-type: none"> - The page is displayed normally - Displays all added 3rd party CTI information in the dashboard after the button is clicked smoothly and efficiently - One-time add success - Generate new blocks and hashes - no error 	<ul style="list-style-type: none"> - The page is displayed normally - After clicking the button, all the added third-party CTI information is displayed in the dashboard but smooth and inefficient - add sequentially - Generate new blocks and hashes - A small number of errors occurred but did not affect functionality 	<ul style="list-style-type: none"> - The page is displayed normally - Display all added third-party CTI information in the dashboard after clicking the button - Generate new blocks and hashes - add sequentially - There are a lot of errors and have an impact on efficiency and smooth 	<ul style="list-style-type: none"> - function not implemented - After clicking the button, the added third-party CTI cannot be displayed in the dashboard - Cannot generate new blocks and hashes
--------------------	--	---	---	--

4 Group Reflection.

a) How your team collectively applied the knowledge from your major units (be explicit in terms of which units' knowledge was referred to and applied to the given problem).

The main judgement for us to find groupmates is that each person needs to have the specific ability to enable the success of the project. In our group there are 6 members from the same faculty but not the same major, we have cyber security, software development, computer science, business analytics and enterprise system, which is easy to contribute to the group. The different technical backgrounds enhance the effectiveness of the project, for instance, Lin(Lin Chen) focuses on the front-end prototype of the project with adobe XD the reason is that she used to study design and accompany Bader to finalise the literature review. Bader mainly responds to the literature review and the CouchDB of the back-end, he is doing well in summarising the article, he also is our scrum master. Sonny(Yuxuan Shen) is the main programmer of this project, he took part in most of the coding requests in this project. Ivy(Xutong Wan) and Daniel(Dongxi Cai) are experts in website programming, especially daniel has the website program experience in Brisbane, while these two mates help with the front-end and back-end connection. Sonny and Vivian(Yijun Xu) have the programming basement to support the back-end task and combination of the whole project artefacts. Also, Vivian is the leader and does project process management. In brief, each member of our group has strong support for the project, effective communication and hard work to help us achieve the goal always.

b) How does your team collaborate to address the problems and issues encountered during the execution.

The prophase of the project plan is that the project scope is not clear for us, our group is still hard working on preparing and program learning, and the step was behind the schedule. Our group has realized the severity of the problem, we just have a face-to-face meeting to catch up which needs each person to read two articles and record the summary update to the platform. Meanwhile, the development has been sped up to make a basic UI design and back-end.

In terms of UI design, our group members have different opinions about the layout, the final version for that is judgement by the percentage of the support, we have deep communication to list the pros and cons to make updates.

The whole process of the project, our group members respected each other, the atmosphere is also active and happy, and we satisfied the group members' attribution and the outcome.

c) If your team completed any research or learned new tools and technologies, you can reflect upon them in terms of new learnings and findings.

New knowledge from

Technology:

Most of the group members did not have a background in networking security, the pandemic also impact our group. Each team member has learned networking field knowledge about blockchain and Hyperledger.

Tool:

The use of the Trello within our group is quite clear know the step,each team member know how to use Trello to update the document, link and activity. The record of the history will give us the power to stimulate the schedule.

Research:

Each team member read enormous articles about the risk of blockchain under 5G to list all the summaries of researchers on the current influence of blockchain technologies. This effectively filled in the research gap that we needed when started the new semester as the majority of our team members came from a non-related background.

d) If there are any group-level challenges faced (time constraints, one member not contributing, non-availability of industry partner or tutor, etc), then how do you address them and took the necessary actions to overcome them.

Our group had six members, so the schedule to accommodate, the parts to delegate, the parts to integrate, etc., was complicated at first.

In the beginning, each team member made a weekly schedule for their available time. We used WeChat as a communication platform, which was convenient and fast and put important itineraries and tasks on Trello.

Then assign roles and have the leader designate times for group meetings and use the group's personal skills checklist to help the team delegate subtasks. The leader will push students through time-consuming phases and tasks and assign time to the group in the project schedule to integrate parts.

e) Experience of working with an industry partner and what were your key learnings for the team.

Collaborating with industry partners to gather information and find the best way to incorporate this information into the curriculum is an invaluable resource for curriculum development. Also, using scenarios in a course is a great way to engage students and help learners acquire knowledge and skills. It is important that any scenarios included accurately describe the situations that will be encountered on the job. Employers are aware of dilemmas or problems that often arise in the work environment and can help create scenarios that realistically describe these situations.

f) What processes and methods were adopted by your team to handle the changes encountered during the project?

We conduct meeting reviews and change assessments immediately after each week with industry partners. To ensure greater project transparency and accountability within the team. Also, hold regular meetings a few times a week to prevent miscommunication or stay on the right track.

5 Reference

- Baker, K. (2022). *What is Cyber Threat Intelligence? [Beginner's Guide]*. crowdstrike.com. Retrieved 14 June 2022, from <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/>.
- Dalziel, H. (2015). How to define and build an effective cyber threat intelligence capability. Syngress, an imprint of Elsevier.
- Moore, R. O. (2021). Cyber intelligence-driven risk : how to build and use cyber intelligence for business risk decisions. John Wiley & Sons, Inc.
- Morville, P., & Sullenger, P. (2010). Ambient findability: libraries, serials, and the internet of things. *The serials librarian*, 58(1-4), 33-38.
- WAEL, A. H. S. A., & SUFYAN, T. F. A.-J. (2019). USING DSDM FOR DEVELOPING GRADUATE STUDY-BASED CRYPTANALYSIS PROJECTS. *i-Manager's Journal on Communication Engineering and Systems*, 8(4), 1—. <https://doi.org/10.26634/jcs.8.4.17105>

6 Appendix

6.1 Team Performance Control


<i>Items</i>	<i>Controls</i>	<i>How to controls work</i>
Time	Project timelines Gantt chartt MoSCow prioritization	Good vision on overall timeline through the project, and control on time efficiency.
Quality	Status report sprint plan	Gives good information about the team and control of the capacity and effort done within the sprint.
Cost	Cost estimation	Effectively allow us to browse costs that will occur through the duration of the project, and delete unnecessary costs that may occur.
Performance	<i>Trello</i> <i>Zoom</i> <i>Wechat</i>	<div></div> <p>Trello is a useful collaboration tool that will give good control of the entire project process, with a good view of the completion process of each member. Zoom can supervise team members in performance in timely manner. Using Wechat to communicate eachothers immediately.</p>

Figure 6.1.1: Performance Control

General team terms:

1. Follow the terms of this document.
2. Only Communicate in English.
3. Ask questions: when we face challenging a task you should not hesitate to ask the team.
4. Respect each other, If someone feels unfair, we need to deal with this situation immediately.
5. Each team member must spend at least 20 hour a week on the project.
6. Everyone has equal voice and valuable contribution
7. Raise a problem as soon as you see it. If you have a question, discuss it with the team first. Then if needed, reach out to the tutor.
8. Exchange knowledge to improve our skills. During the weekly meetings, team members may share useful resources regarding the project.
9. Always give positive feedback and avoid personalising issues.
10. Keep learning. Many free courses are available on linkedin learning and Youtube.

Communication terms:

1. All team members need to use WeChat as first communicating platform then by Email, Trello or phone call.
2. respond to messages as soon as possible.
3. Keep Trello board updated. Add or comment on tasks as needed.

Documentation terms:

1. All team documents must be shared to all teammates via google drive folder.
2. Each meeting must be documented and summarised.
3. Document your individual weekly progress, as you will need it later for the reflection.

Meetings terms:

1. All team members must attend all meetings. If not, inform other teammates before the meeting date. And as the case may change to online meetings.
2. Be on time during each meeting.
3. come prepared to meetings and tutorials
4. Meet twice a week. Once before the tutorial to prepare for the weekly materials, and once for check the weekly tasks process.

Figure 6.1.2: Team Contract

6.2 Functional and nonfunctional requirements

Area/Deliverables	Domains	Functional requirements	Complexity	Effort estimations
Client Application (index page/consumer page/contributor page)	identity management	Instantiate a CTI information sharing platform	Medium	20 hour
	Network Contract Development	Register/Log in	High	80 hour
		Manage identity	High	50 hour
		Create and use a connection profile	Medium	20 hour
		Instantiate and connect a gateway	Medium	20 hour
		Access network and contracts	High	60 hour
Chaincode (docker containers/fabric network file)	Smart contract development	Define smart contract construct	Medium	20 hour
		Define transaction function	High	80 hour
		implement deterministic code/logic	Medium	20 hour
		Create queries	High	50 hour
		initialization of the ledger state	Low	10 hour
	Smart contract invocation	Instantiate a smart contract	Medium	20 hour
		Invoke smart contracts via CLI	Medium	20 hours
		transaction function: queries	High	50 hours
		transaction function: add	High	50 hours
		register and handle channel-based event	High	30 hours
Test plan (final report)	Handle error and success responses		Medium	20 hours
	identify and review logs		Medium	20 hours
	test smart contracts		High	60 hours
	Diagnose and endorse policy conflicts		Medium	20 hours
	troubleshoot transaction flow		Medium	20 hours

Chaincode (docker containers/ fabric network file)		Instantiate and connect a gateway	Medium	20 hour
		Access network and contracts	High	60 hour
	Smart contract development	Define smart contract construct	Medium	20 hour
		Define transaction function	High	80 hour
		implement deterministic code/logic	Medium	20 hour
		Create queries	High	50 hour
		initialization of the ledger state	Low	10 hour
	Smart contract invocation	Instantiate a smart contract	Medium	20 hour
		Invoke smart contracts via CLI	Medium	20 hours
		transaction function: queries	High	50 hours
		transaction function: add	High	50 hours
		register and handle channel-based event	High	30 hours
Test plan (final report)		Handle error and success responses	Medium	20 hours
		identify and review logs	Medium	20 hours
		test smart contracts	High	60 hours
		Diagnose and endorse policy conflicts	Medium	20 hours
		troubleshoot transaction flow	Medium	20 hours

Figure 6.2.1 : Functional Requirements

Area/Deliverables	Domains	Functional requirements	Complexity	Effort estimations
Client Application (index page/consumer page/contributor page)	identity management	Instantiate a CTI information sharing platform	Medium	20 hour
	Network Contract Development	Register/Log in	High	80 hour
		Manage identity	High	50 hour
		Create and use a connection profile	Medium	20 hour

Figure 6.2.2: Nonfunctional Requirements

6.3 Risk management

ID	Cause	Risk	Resulting in	Impact low/medium/high	How to prevent it?
R1	lack of involvement in the learning stage of the project	Lack of knowledge of the project requirements.	Rework later and increase pressure load later on.	High	Commitment and early learning
R2	Lack of ownership	Lack of motivation	Poor quality deliverables	High	Remember that this research could help many organisations to prevent attacks which is a novel cause
R3	Lack of responsibility or knowledge	Unable to complete allocated tasks	Delay of deliverables or not meeting project requirements	Medium	Weekly checks on team progress.
R4	lack of cooperation between members	Lead to low work efficiency	Misunderstanding allocated task	Medium	Pay attention at meetings and cooperate
R5	Insufficient time and resources to propose new applications to project stakeholders,	Insufficient knowledge and technology make it difficult to make changes immediately	The program has an exception and cannot be implemented	high	Find more academic reports and do literature reviews
R6	lack of literature review	Lack of understanding of new knowledge	Influence the progress of the project and cannot cooperate with others	Medium	Spend more time doing literature reviews
R7	Not familiar with programming	The coding phase of	When coding, the efficiency is	Medium	Learn the official documentation and

	languages	the project is difficult to complete	low and there are many bugs		view related videos-Yuxuan Shen
R8	Unable to attend the meeting due to some unavoidable emergencies	May be unable to keep up with the process	Inability to understand specific tasks and goals	Medium	Ask the team leader or other team members about the content of the meeting and record it-Yuxuan Shen
R9	Lack of communication between the stakeholders	Loss of interest in project	Demotivation from all parts	Low	Keep communicating with

		Impact		
		L	M	H
Likelihood	L		R3	R5
	M	R9	R7	R2
	H		R6, R8, R4	R1

Figure 6.3.1: Risk management

6.4 Burndown chart

