Week 1 – Introduction to the Unit and Blockchain

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Unit Overview

What this unit is about?

This is a project-based unit where students collaborate in teams to develop innovative solutions for industry challenges.

What are you going to learn?

The primary focus of this project is to apply a range of IT techniques and analysis methods to effectively address these challenges

How much time do you need to dedicate to studying?

- Watch seminar video: 1 hr
- Watch live lecture video: 1hr
- Attend and participate in the workshop : 2 hrs
- Complete the post_class activities and assessments: Approx. 8 hrs

How to pass the unit?

All assessments for this unit will be handled in the semester, and there are a total of 3 group assignments, which will make up 100% of the unit's mark, implying no exam. (Please consult Canvas for more details on all assessments.)

In order to pass, your unit total must be over 50%, or 50 out of 100 marks.

SWINBURNE UNIVERSITY OF TECHNOLOGY

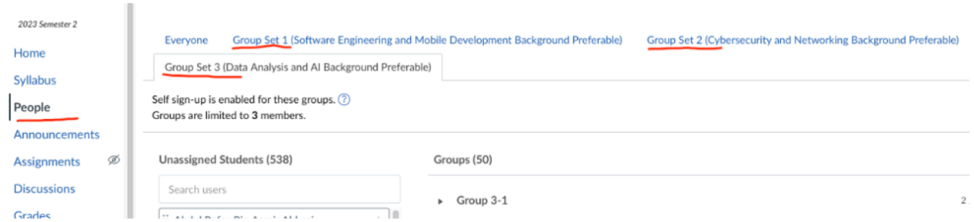
Group Sets

This unit is a large team-based course that brings together students with diverse backgrounds. To ensure an optimal learning experience, we have designed three distinct group sets for the students, each catering to specific preferences and expertise. They are as follows:

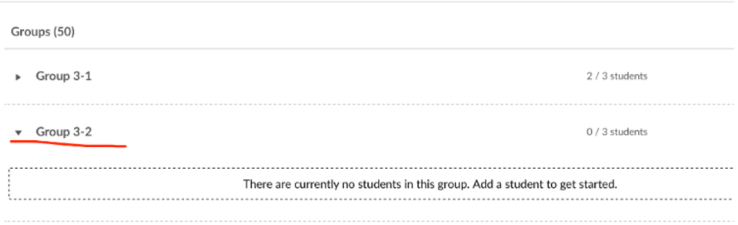
- Group set 1 (Software Engineering and Mobile Development Background Preferable),
- Group set 2 (Cybersecurity and Networking Background Preferable), and
- Group set 3 (Data Analysis and AI Background Preferable).

Every student is required to register for one group from a predefined set, with each group comprising **three** students.

Step 1: go to People section, and select a group set.



Step 2: To join a group from the list, simply select the one that best aligns with your preferences and click to confirm your choice. Feel free to switch between different groups until you find the right fit. However, please note that once you have submitted the first assignment, group changes will no longer be allowed. Within each group, one student will be designated as the group leader, responsible for coordinating and leading the team's projects.



Projects Overview

For students with ***Software Engineering and Mobile Development Background*** this project is about:

- This decentralized trading platform is built on blockchain technology, aiming to ensure transparency and security of user transaction information. Through the immutability and distributed nature of blockchain, each transaction is recorded on the blockchain, making transaction data openly transparent and tamper-proof.

- The platform's website will be designed with a responsive layout to ensure a seamless browsing experience for users across different devices. The system's backend will be developed using Node.js, a popular server-side runtime environment known for its outstanding performance and scalability. Meanwhile, the functionality to interact with smart contracts and the blockchain network will be implemented using Ether.js, a specialized JavaScript library for Ethereum blockchain interactions.

- For students, they are required to design smart contract functions according to their specific needs. This means they can write smart contract functions based on the platform's specific business logic and requirements, such as implementing asset exchange, transfer functionalities, or adding other custom features to meet user demands. Safety and effectiveness should be thoroughly considered in the design of smart contracts to ensure reliable execution of transactions and protection of user data.

In summary, this decentralized trading platform utilizes blockchain technology to ensure transparency of transaction information. The website is designed with a responsive layout, and the backend is developed using Node.js. Students are responsible for designing smart contracts according to their needs and requirements.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Projects Overview

For students with ***Cybersecurity and Networking Background*** , this project is about:

- The Smart Contract Vulnerability Detection Platform aims to assist users in identifying potential vulnerabilities in smart contract code. The platform provides a responsive website that allows users to upload their smart contract code. By utilizing existing smart contract static analysis tools, the platform can rapidly analyze the contract code and identify potential issues. Users can view the detection results on the website, enabling them to promptly identify and address any vulnerabilities in their contracts.

- The adaptive website design ensures seamless usability across different devices. Users simply need to upload their smart contract code, which will be submitted to the static analysis tool for examination. The tool will identify potential problems such as security vulnerabilities, code errors, or other risks, and display the results on the website for users to review.

- This Smart Contract Vulnerability Detection Platform offers a convenient solution for smart contract developers to ensure the quality and security of their code. By timely detecting potential vulnerabilities, developers can prevent security issues that might lead to losses and enhance the trustworthiness and reliability of their contracts. The platform contributes to the healthy development of the smart contract ecosystem, safeguarding the interests of both users and developers.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Projects Overview

For students with ***Data Analysis and AI Background***, this project is about:

- The Blockchain Transaction Information Visualization Platform is a solution designed to visualize blockchain transaction data. The main functionalities of this platform include crawling transaction data from specified block data, data tagging, and importing into the Neo4j graph database. Users can access and explore the processed data through the website's backend, enabling them to visualize transaction information.

- To begin with, the platform crawls transaction data from specified block data, retrieving essential information such as transaction sender, receiver, amount, and timestamp from the blockchain network. The collected data then undergoes a series of processing steps. Next, the platform tags the obtained transaction data. Through data tagging, the platform categorizes and links transactions, facilitating the identification of different transaction types and the discovery of potential patterns or anomalies.

- Subsequently, the processed transaction data is imported into the Neo4j graph database. The advantage of using a graph database lies in its ability to efficiently store and query complex relationships. In Neo4j, the transaction data is structured into nodes and relationships, forming a graph.

- Through the website's backend, users can access the Neo4j graph database and visualize transaction information. The platform may offer various visualization methods, such as graphical displays and chart analyses. Users can select the most suitable visualization method based on their needs, enabling a better understanding and analysis of blockchain transaction information.

In summary, the Blockchain Transaction Information Visualization Platform effectively handles and visualizes blockchain transaction data through crawling, tagging, and importing into a graph database. It offers users an intuitive and convenient way to comprehend and analyze blockchain transaction information, facilitating the discovery of potential transaction patterns and anomalies. This platform serves as a valuable reference for further optimization and improvement of blockchain applications.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assignments

This year, we select web3 as the working platform to design/introduce real-world projects into this unit.

There will be around nine different small projects tailored for students who may have different backgrounds.

For each group set, the three consecutive projects are listed below:

For group set 1, which prefers students that have software engineering background, we have

- Assignment 1-1: Decentralised Trading Platform - Static Website (Front-end) (weight: 30%),
- Assignment 1-2: Decentralised Trading Platform - Dynamic Website (Back-end) and Smart Contract Development (weight: 40%),
- Assignment 1-3: Smart Contract Code Review and Illustration Report (weight: 30%).

For group set 2, which prefers students that have cybersecurity background, we have

- Assignment 2-1: Security Auditing Platform - Static Website (Front-end) (weight: 30%),
- Assignment 2-2: Security Auditing Platform - Dynamic Website (Back-end integrated) and Application of Contract Audit Tools (weight: 40%),
- Assignment 2-3: Security Case Study and Auditing Report (weight: 30%).

For group set 3, which prefers students that have data analysis and AI background, we have

- Assignment 3-1: Transaction Tracing Platform - Static Website (Front-end) (weight: 30%),
- Assignment 3-2: Transaction Tracing Platform - Dynamic Website (Back-end integrated) (weight: 40%),
- Assignment 3-3: Transaction Analysis and Tracing Report (weight: 30%).

Overview of Blockchain Technology

- **Definition of a blockchain:** A digital, distributed, and decentralized ledger that records transactions across multiple computers.
- **Security:** Blockchain uses advanced cryptography to secure transactions and prevent unauthorized access.
- **Transparency:** All transactions are visible to every participant in the network, ensuring openness and trust.
- **Immutability:** Once a transaction is recorded on the blockchain, it cannot be altered or deleted, ensuring data integrity.
- **Decentralization:** No single entity controls the blockchain; instead, control is distributed among all participants in the network.

Key Concepts in Blockchain

- **Blocks:** The data structure that stores a set of transactions, linked to previous blocks to form a chain.
- **Transactions:** The transfer of data or assets between participants in the network, validated by nodes.
- **Nodes:** Computers in the network that validate and relay transactions, maintain a copy of the entire blockchain, and enforce consensus rules.
- **Consensus Mechanisms:** Rules and processes that nodes follow to agree on the contents of the blockchain.
- **Proof of Work (PoW) vs. Proof of Stake (PoS):** Two popular consensus mechanisms with different approaches to validating transactions and securing the network.

Introduction to Ethereum

- **Ethereum:** A decentralized, open-source, blockchain platform that enables the creation of smart contracts and decentralized applications (DApps).
- **Purpose:** To provide a platform for developers to build and deploy decentralized applications using smart contracts.
- **Ether (ETH):** The native cryptocurrency used to power transactions and smart contracts on the Ethereum network.
- **Ethereum Virtual Machine (EVM):** A runtime environment that processes and executes smart contracts on the Ethereum network.

Ethereum vs. Bitcoin

- **Purpose:** Bitcoin is primarily a digital currency, while Ethereum enables the creation of decentralized applications and smart contracts.
- **Use Cases:** Bitcoin is mainly used for transferring value, whereas Ethereum supports a broader range of applications.
- **Scalability:** Both Bitcoin and Ethereum face scalability challenges, but Ethereum is working on various solutions like Ethereum 2.0 and Layer 2 technologies.
- **Consensus Mechanisms:** Bitcoin uses Proof of Work, while Ethereum is transitioning from Proof of Work to Proof of Stake with Ethereum 2.0.

Smart Contracts

- **Definition:** Self-executing contracts with the terms of the agreement directly written into code, automatically executed when predetermined conditions are met.
- **Benefits:** Reduced transaction costs, increased trust, automation, and security.
- **Creating Smart Contracts on Ethereum:** Developers can write smart contracts using Solidity, a programming language specifically designed for Ethereum.
- **Solidity:** A high-level, statically-typed programming language designed for writing smart contracts on the Ethereum platform.

Use Cases of Ethereum

- **Decentralized Finance (DeFi):** Financial applications built on Ethereum that aim to democratize access to financial services.
- **Non-Fungible Tokens (NFTs):** Unique digital assets representing ownership of digital or physical items, powered by Ethereum's ERC-721 and ERC-1155 standards.
- **Decentralized Autonomous Organizations (DAOs):** Organizations governed by smart contracts and community consensus, rather than a centralized authority.
- **Supply Chain Management:** Tracking and verifying the provenance and movement of goods through a transparent and secure blockchain.
- **Identity Management:** Decentralized systems for managing digital identities, enabling user control and privacy.

Thank You