



TUNKU ABDUL RAHMAN UNIVERSITY OF MANAGEMENT AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY






**BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN INFORMATION SECURITY
2024/2025**

RIS 3 SEM 1 (GROUP 3)

Written Assignment

BACS3033 Social and Professional Issues

Semester 202405

Student Name (Block Capital)	Registration No.	Signature	Final Mark
1. WHELAN YAP BOON HONG	23WMR02180		
2. PANG JIN SIANG	23WMR11552		
3. LEE KONG HANG	23WMR00399		
4. LIM YING THONG	23WMR00727		
5. ONG EN TING	23WMR03170		

Tutor's Name: **Ms Goh Kim Nee**

Date of Submission: **9 September 2024**

**Faculty of Computing and Information Technology****Plagiarism Statement**

Read, complete, and sign this statement to be submitted with the written report.

We confirm that the submitted work are all our own work and are in our own words.

	Name (Block Capitals)	Registration No.	Signature
1.	<u>WHELAN YAP BOON HONG</u>	<u>23WMR02180</u>	
2.	<u>PANG JIN SIANG</u>	<u>23WMR11552</u>	
3.	<u>LEE KONG HANG</u>	<u>23WMR00399</u>	
4.	<u>LIM YING THONG</u>	<u>23WMR00727</u>	
5.	<u>ONG EN TING</u>	<u>23WMR03170</u>	

Programme & Tutorial Group : RIS 3 Sem 1 Group 3

Date : 4 September 2024



BACS3033 Social and Professional Issues

Individual Tasks Allocation

Indicate (√) in member name column if he/she have involved in that task.

Tasks		WHELAN YAP BOON HONG	PANG JIN SIANG	LEE KONG HANG	LIM YING THONG	ONG EN TING
1.	Background	√		√		
2.	Finding (Social)		√		√	√
3.	Finding (Legal)	√		√		√
4.	Finding (Architectural)		√	√	√	√
5.	Finding (Market)	√	√		√	
6.	Solution (Social)		√	√		√
7.	Solution (Legal)	√			√	
8.	Solution (Architectural)	√		√	√	√
9.	Solution (Market)		√			
10.	Individual Assignment	√	√	√	√	√

FORM 2

Assignment Final Report Assessment Criteria

CLO2: Write an in-depth finding and justification on contemporary issues in computing through written report.

CLO3: Present the basics of ethics in the field of computing.

Group Assessment

Assignment Marking (Part 1) (70%)					
Criteria	Excellent	Good	Average	Poor	Score
(a)Background (4%) CLO2	Very clear description about the background of the contemporary topic selected.	Some part of description about the background of the contemporary topic selected with ambiguity.	Brief description about the background of the contemporary topic selected, which are not directly related to question.	Very brief description about the background of the contemporary topic selected, which are not related to question.	
	(4%)	(3%)	(2%)	(0-1%)	
(b) Finding +Justification of the chosen topic from social, legal, architecture and market perspectives. (40%) CLO2	Able to provide very clear and reasonable assessment & justification with very details explanations on the chosen topic from social, legal, architecture and market perspectives. Able to look for relevant information independently from many sources within the duration of time given and well utilize it.	Good to provide reasonable assessment & justification on the chosen topic from social, legal, architecture and market perspectives. However, some explanations are not clear. Able to look for relevant information independently from many sources but some information is not used wisely.	Average to provide reasonable assessment & justification with limited explanation on the chosen topic from social, legal, architecture and market perspectives. Able to look for information independently from many sources but some of them are irrelevant or sometimes can only use them with some assistance from others.	Poor to provide reasonable assessment & justification with very little to no explanation at all on the chosen topic from social, legal, architecture and market perspectives. Able to look for very limited information independently and subject to limited few sources and majority information are irrelevant.	
	(31-40%)	(21-30%)	(11-20%)	(1-10%)	

(c) Proposal of the solution(s) upon your chosen topic from social, legal, architecture and market perspectives. (20%) CLO2	Able to provide very clear and reasonable evaluation with very details explanations on the proposal of the solution(s) upon your chosen topic from social, legal, architecture and market perspectives. Able to apply excellent new ideas and thoughts in solutions perfectly at all situations.	Good to provide reasonable evaluation on the proposal of the solution(s) upon your chosen topic from social, legal, architecture and market perspectives. However, some explanations are not clear. Able to apply good new ideas or thoughts in solutions in most situations.	Average to provide reasonable evaluation with limited explanation on the proposal of the solution(s) upon your chosen topic from social, legal, architecture and market perspectives. Able to apply some new ideas or thoughts in solutions under certain situations.	Poor to provide reasonable evaluation with very little to no explanation at all on the proposal of the solution(s) upon your chosen topic from social, legal, architecture and market perspectives. Unable to propose & unable to apply new ideas or thoughts on solution.	
	(16-20%)	(11-15%)	(6-10%)	(1-5%)	
Independent Learning and Self explorative Skills (6%) CLO 2	Able to conduct Independent Learning and explore the topic selected well. Work shows a large amount of original thought and complete on time with very little/no supervision and exceeds expectation. Ideas are creative and inventive.	Able to conduct Independent Learning and explore the topic selected in a fair manner. Work shows some original thought and complete on time with little supervision and overall meet expectation. Some works show new ideas and insights with some other part of works use other people's idea.	Able to conduct Independent Learning and explore the topic selected averagely. Work shows little original thought and with close supervision and sometimes not meet expectation. Uses other people's ideas/work and little evidence of original thinking.	Poor to conduct Independent Learning and explore the topic selected poorly. Work shows no/very little original thought even with close supervision and not meet expectation. Mainly uses other people's ideas/work.	
	(6%)	(4-5%)	(2-3%)	(0-1%)	
Sub-Total (70%)					

Assignment Marking (Part 2) (30%)				
Criteria	Excellent	Good	Average	Poor
(d) Reflective Writing -- Identification and justification of ethical issues from chosen topic with appropriate selection of the ethics philosophy to support it (30%) CLO 3	Able to provide very clear and reasonable assessment of ethical issues raised from chosen topic. Excellent justification on such ethical issues with well appropriate selection of the ethics philosophy to support it. Able to give excellent interpretations and consider numerous views from related perspectives based on facts, rules and laws that are relevant to the ethical problem.	Able to provide clear and reasonable assessment of ethical issues raised from chosen topic. Good justification on such ethical issues with well appropriate selection of the ethics philosophy to support it. However, some explanations are not clear. Able to verify whether the facts are relevant or not based on facts, rules and laws relevant to the ethical problem.	Average to provide clear and reasonable assessment of ethical issues raised from chosen topic. Average justification on such ethical issues with limited point to support it. Able to gather facts related to ethics problem but some of it being irrelevant.	Poor to provide clear and reasonable assessment of ethical issues raised from chosen topic. Poor justification on such ethical issues with very limited or no point to support it.
	(24-30%)	(16-23%)	(8-15%)	(1-7%)
Whelan Yap Boon Hong				
Pang Jin Siang				
Lee Kong Hang				
Lim Ying Thong				
Ong En Ting				
Sub-Total (30%)				

Student Name	Group Assessment	Individual Assessment	Total Marks
Whelan Yap Boon Hong			
Pang Jin Siang			
Lee Kong Hang			
Lim Ying Thong			
Ong En Ting			

Lecturer/Tutor's Feedbacks/Comments:

Table of contents

Background	1
Components of Blockchain	1
Stakeholders of Blockchain	2
Group Work	3
Social Perspective	3
Legal Perspective	5
Architectural Perspective	7
Market Perspective	9
Group Work	11
Social Perspective	11
Legal Perspective	12
Architectural Perspective	13
Market Perspective	14
Terra Blockchain Security Breach (Whelan Yap Boon Hong)	15
Cause of Security Breach	15
Stakeholders Involved	15
Ethical Considerations	15
Beliefs & Values	16
Attitudes & Assumptions	16
Mixin Network Security Breach (Pang Jin Siang)	17
Cause of Security Breach	17
Stakeholders Involved	17
Ethics Philosophies	17
Value	18
Attitudes	18
Assumptions	18
Binance Cryptocurrency Theft Incident (Lee Kong Hang)	19
Cause of Cyber Attack	19
Stakeholders Involved	19
Ethical Considerations	19
Beliefs & Values	20
Attitudes & Assumptions	20
Ronin Network Hack (Lim Ying Thong)	21
Cause of Security Breach	21
Stakeholders Involved	21
Ethical Considerations	21
Beliefs & Values	22
Attitudes & Assumptions	22
Poly Network Hack (Ong En Ting)	23
Cause of Security Breach	23
Key stakeholders in this incident included:	23
Ethical Considerations	24
Beliefs & Values	24
Attitudes & Assumptions	24
References	25

Background

The concept of blockchain was introduced in 2008 along with the invention of Bitcoin. It was implemented for practical use in 2009 (*Bashir. I, 2017*), which was with the Bitcoin cryptocurrency. It plays the role of a decentralized consensus mechanism, which allows information collection & storing when an entity buys, sells, or exchanges cryptocurrency (*Coursera, 2023*).

Blockchain is a chain of blocks, whereas the “block” is added to a “chain” of blocks. “Block” refers to the data stored while “chain” refers to the database. Cryptography is used to link the blocks together by using hash pointers that point to the previous block (*Bashir. I, 2017*). Each block consists of a cryptographic hash of the previous block for security purposes such as preventing data alteration or deletion.

Components of Blockchain

Blockchain consists of multiple components that play their role in storing & securing data. The key components of blockchains are blocks, hash codes, nodes, ledgers, & nonce (*Saikumar. K, 2023*).

Blocks

Blocks store data & are arranged in chronological order. After the data is stored, the chance to alter the block data is near zero. Data change can still be performed but it is unlike any typical data change. The way blockchain performs data change is by adding a new block with the new changes to another block and linking it to the respective existing old block.

Hash Codes

Hash codes act as the blockchain’s security measure. It converts the input data into bytes in a fixed length regardless of the input’s length. This form of security layer ensures that the blockchain cannot be cracked or altered easily while also not being detected. This is due to the block header of every block that has the previous block header’s hash.

Nodes

Nodes can be defined as the data storage of a blockchain. For instance, a computer system is a node to store data. The blockchain network connects all the nodes & can detect changes made in the blockchain data.

Ledgers

Ledgers are mechanisms that help to keep the record of a blockchain. It is a record of transactions & data stored digitally in a distributed manner across several nodes globally. All nodes in the blockchain network have copies to ensure transparency & accuracy of information (*Shoemaker. P, 2023*).

Nonce

Nonce refers to a one-time use only value to authenticate users. Whenever a new block is created or during the validation of a new transaction, a nonce will be generated. It is used with the hashed blocks to rehash the block’s hash value, making it harder to crack the algorithm.

Stakeholders of Blockchain

The stakeholders in blockchain vary depending on the type of blockchain application. The primary stakeholders are miners, node operators, developers, users, governance entities, and investors & speculators. They contribute to the overall functioning & security of the blockchain ecosystem (*FasterCapital, 2024*).

Miners

Miners solve challenging mathematical puzzles to validate transactions & add new transactions to the blockchain. Cryptocurrency tokens are given to them as a reward for their efforts.

Node Operators

Node operators take part in the consensus process & validate transactions to ensure the integrity of the blockchain ledger while also maintaining its copies.

Developers

Developers play the role of creating & maintaining the blockchain software, implementing new features, & bugs fixing. Their involvement contributes to the improvements & evolution of the blockchain.

Users

Users perform transactions & engage in the usage of the blockchain ecosystem. They contribute to the growth of the blockchain by participating in network activities.

Governance Entities

Governance entities make decisions on blockchain network's regulations, upgrades, & community governance. They ensure that the blockchain network runs transparently & fairly by taking the interest of all parties involved into account.

Investors & Speculators

Both parties support blockchain projects financially by contributing capital for development, selling tokens, & trading cryptocurrencies on exchanges. Their involvement sustains the blockchain & can impact the success of the blockchain.

[630 Words]

Explore and analyze your chosen topic from social, legal, architecture and market perspectives. [40 marks]

Analyze the selected topic with examples, case studies, facts, etc to provide your finding here. Justify your opinions/thoughts on the impacts of selected topic from social, legal, architecture and market perspectives.

Group Work

Social Perspective

The promise of blockchain technology to improve transparency and democratize access to financial services makes it a significant social technology. Peer-to-peer transactions made possible by blockchain's elimination of middlemen promote inclusivity for those without access to traditional financial institutions (**Kshetri, 2021**). For example, BitPesa and other blockchain-based platforms have transformed cross-border transactions by making them more affordable, easier, and efficient. With BitPesa, users in African nations may send and receive money fast without having to deal with the expensive fees and protracted processing periods that come with using traditional banks and remittance services (**Kisawuzi, 2023**).

Moreover, the transparency provided by blockchain has the potential to fight corruption, especially in areas where corruption is common and weakens public trust. Blockchain technology generates a tamper-proof, verifiable record of transactions that can be audited at any moment by creating an immutable ledger. Due to the importance of accountability and openness, this competence can be very helpful in public sector initiatives and government contracts. To cut down on fraud and boost transparency in real estate transactions, the Georgian government, for example, has introduced a land registration system based on blockchain technology (**Anconia, 2017**).

Governments and regulatory organizations worldwide are putting more and more effort into creating thorough regulatory frameworks for blockchain technology in order to address the anonymity crime issues. These frameworks aim to balance the need for security and transparency with the innovation potential. For example, the Financial Action Task Force (FATF) has issued guidelines for anti-money laundering (AML) and combating the financing of terrorism (CFT) that apply to virtual assets and service providers (**FATF, n.d., 2024**), (**IMF, 2023**). According to these regulations, companies that use blockchain technology must establish know-your-customer (KYC) procedures and notify the appropriate authorities of any questionable activity.

In conclusion, blockchain technology has a lot of potential to improve fairness and transparency in many areas. It can make financial services more accessible by allowing peer-to-peer transactions without middlemen, especially where traditional banks are not available. Blockchain's transparency can help fight corruption in government and supply chains, building more trust. However, its anonymity means strong regulations are needed to prevent illegal activities. To fully benefit from blockchain, it's important to balance innovation with regulation as the technology evolves.

Challenges of Implementing Blockchain in Social Perspective

Blockchain's promise of anonymity and privacy can also present significant social challenges. Although blockchain's anonymous feature can safeguard user privacy and provide security advantages, it also opens doors for illegal operations including fraud, money laundering, and other illicit transactions (*Dulani Woods et al., 2023*).

Criminals can use the anonymous features of blockchain to commit crimes without being easily identified. It is essential to create strong legal rules to reduce these risks and keep the benefits of blockchain. For instance, the 2014 Mt. Gox scandal revealed how vulnerabilities and the anonymous nature of blockchain could be exploited, leading to the theft of approximately 850,000 Bitcoins, which highlighted the urgent need for improved security measures and regulatory oversight (*Team, 2024*).

[468 Words]

Legal Perspective

Blockchain technology offers transformative potential for various sectors, including the legal field, by providing innovative solutions for contract management and transaction transparency. The decentralized nature of blockchain enables direct, peer-to-peer interactions without the need for traditional intermediaries. This characteristic enhances efficiency and reduces the risks of fraud and errors. For example, blockchain-based smart contracts automate and enforce agreements by encoding terms directly into code, significantly improving transaction reliability and reducing administrative overhead. Platforms like Ethereum lead in this technology, revolutionizing industries such as supply chain management, insurance, and real estate.

For instance, blockchain-based smart contracts streamline real estate transactions by automating tasks like payment processing and contract execution (*LLC, 2024*). This reduces reliance on escrow agents and other intermediaries, minimizing errors and disputes. In insurance, smart contracts automate claims processing based on predefined criteria, boosting efficiency and reducing administrative costs. Moreover, blockchain enhances transparency and traceability in supply chain management transactions, improving accountability and reducing fraud.

Governments and regulatory organizations are exploring ways to harness the benefits of blockchain while minimizing risks. Initiatives such as the FATF recommendations on virtual assets aim to enhance regulatory oversight to prevent money laundering and terrorist financing (*FATF, n.d.*). It is challenging to enforce regulations due to blockchain's decentralized nature since transactions can occur across jurisdictions with different legal standards, despite these attempts. Global enforcement and compliance activities are made more difficult by the fragmented regulatory landscape this produces. A uniform and functional legal framework for blockchain technology must be established to address these issues, which calls for international cooperation and regulatory harmonization.

In conclusion, blockchain technology presents transformative opportunities for enhancing legal processes through automation and transparency. Smart contracts offer efficient alternatives to traditional contract management, revolutionizing industries and improving transaction efficiency. However, legal challenges related to data privacy, regulatory compliance, and dispute resolution must be carefully addressed to fully realize the potential of blockchain technology across various sectors. Finding a balance between innovation and regulation will be critical in shaping the future adoption and integration of blockchain in legal frameworks worldwide.

Challenges of Implementing Blockchain in Legal Perspective

Integrating blockchain into existing legal frameworks requires addressing several key issues. The immutability of blockchain transactions poses challenges for liability and dispute resolution. Since blockchain records cannot be altered, determining legal responsibility for fraud or errors in smart contracts becomes complex. Additionally, robust frameworks are essential for regulatory compliance in sectors such as finance and healthcare. These frameworks must ensure data security, protect consumers, and adhere to specific industry regulations (*Ma & Wales, n.d.*).

Another major challenge is the decentralized nature of blockchain technology, which complicates regulation, particularly concerning cross-border transactions and anonymous identities (*Consensys, n.d.*). Unlike traditional systems, blockchain operates without a central

authority, making it difficult for regulatory bodies to enforce laws and standards consistently. This decentralization challenges legal systems that rely on centralized entities to mediate and enforce regulations. As a result, addressing issues such as jurisdiction and accountability becomes complex, requiring innovative legal approaches to regulate this emerging technology effectively.

Moreover, The General Data Protection Regulation (GDPR) adds another layer of complexity to blockchain regulation. GDPR's stringent data protection requirements are at odds with the immutable nature of blockchain's ledger, particularly concerning the "right to be forgotten" (*Simmons, n.d.*). The GDPR mandates that individuals have the right to request the deletion of their data, but blockchain's permanent record-keeping makes this process challenging. Reconciling the need for data protection with blockchain's immutability presents a significant regulatory hurdle, highlighting the difficulty in aligning modern privacy laws with emerging technologies operating on fundamentally different principles.

[573 Words]

Architectural Perspective

Blockchain technology has transformed digital transactions by creating decentralized, transparent, and secure systems for handling data and transactions (*Baftjari, 2024*). A prime example is Bitcoin, introduced in 2009, which operates as a decentralized digital currency allowing peer-to-peer transactions without intermediaries like banks (*Hayes, 2023*). This innovation has significantly impacted the financial sector by providing a secure and transparent method for conducting digital transactions. The worldwide blockchain market is projected to increase from USD 3.0 billion in 2020 to USD 39.7 billion by 2025, illustrating blockchain technology's significant impact across multiple industries (*Reportlinker, n.d.*).

Decentralization is a core principle of blockchain, where data is distributed across multiple nodes instead of being centralized in one location. This shared ledger system ensures data clarity and makes tampering or fraud extremely difficult. For instance, Ethereum is a decentralized platform that enables developers to build and deploy smart contracts and decentralized applications (DApps). Its decentralized nature guarantees that applications run as programmed without the risk of downtime, censorship, fraud, or third-party interference.

Blockchain's decentralized nature ensures that anyone with network access can view all transactions or data stored on the blockchain. This transparency promotes trust among participants and stakeholders because they can independently verify the accuracy and integrity of the data. For instance, IBM Food Trust utilizes blockchain to improve food safety by offering transparency and traceability in the food supply chain. This enables stakeholders like farmers, processors, distributors, and retailers to access trustworthy information and track the origins of food products instantly. As a result, it helps minimize risks related to food fraud and contamination (*IBM, n.d.*).

Blockchain technology provides a high level of security by storing data in blocks linked in a chain with cryptographic hashes. In order to prevent unauthorized altering, consensus techniques like Proof of Work (PoW) and Proof of Stake (PoS) ensure that only valid transactions are added to the blockchain. Bitcoin's PoW mechanism requires miners to solve complex mathematical problems to validate transactions, making it extremely difficult and resource-intensive for malicious actors to alter transaction data.

Once data is recorded in a block and added to the blockchain, it is extremely difficult to alter or delete. Each block contains a cryptographic hash of the previous block, so any change in one block's data would alter its hash and disrupt the hash sequence, alerting the network to the tampering attempt. This immutability is crucial in sectors like healthcare. For instance, Medicalchain is a blockchain-based platform that securely stores and transfers medical records (*Medicalchain, 2022*). Once patient data is entered into the blockchain, it cannot be altered or deleted, ensuring the integrity and accuracy of medical records.

From an architectural perspective, blockchain technology represents a paradigm shift towards decentralized systems that ensure data integrity, transparency, and security. Its innovative design, leveraging cryptographic techniques and consensus mechanisms, not only enhances trust but also introduces new possibilities for secure digital transactions across diverse industries. As blockchain continues to evolve, its architectural principles will likely shape future developments in technology, offering robust solutions for addressing complex challenges in data management and transactional integrity.

Challenges of Implementing Blockchain in Architectural Perspective

Interoperability is one of the main issues with blockchain technology. Many projects operate on various standalone blockchain platforms, each with its own distinct rules, programming languages, consensus mechanisms, and privacy measures. This fragmentation creates disorder in the blockchain sector, as there are no common standards to link different networks together seamlessly. As a result, data exchange and transactions between disparate blockchains become cumbersome and inefficient. Without consistent protocols, crucial aspects such as security, scalability, and user experience are compromised, hindering the potential for widespread adoption. Furthermore, the lack of interoperability makes it difficult for developers to create applications that can work across multiple blockchain networks, thereby limiting innovation and collaboration within the industry (*Build My Dapp LLC, 2024*).

[613 Words]

Market Perspective

Benefits & Use Cases

The introduction of blockchain technology has revolutionized the digital marketing landscape with its decentralized nature, making it a game-changer for marketers by offering unheard-of levels of security & transparency (*Chirag, 2024*).

In the field of digital marketing, blockchain has enabled **efficient & accurate ad targeting**. The user's data & preferences can be verified precisely to ensure that the advertisements are able to reach the intended target audience, optimizing marketing efforts in terms of exposure & cost spent for the ads, achieving better ROI. One of the use cases involves PepsiCo using Zilliqa's blockchain platform to improve their advertising process by comparing the results of their usual advertising budget with the one that utilized the blockchain technology to see the difference. As a result, the blockchain trial brings a 28% boost in supply chain efficiency in terms of ad impression & the cost, due to the use of smart contracts (*Khatari, 2019*).

Blockchain consists of digital tokens that are issued by each participant in the supply chain to authenticate its movement, making it possible to **trace the source of goods** (*McDaniel, 2019*). This provides transparency & accuracy of a product's journey to the store, ensuring the authenticity of the goods while building the trust of consumers by letting them know the information is unaltered. Nestlé is one of the companies that utilizes blockchain technology by collaborating with OpenSC's blockchain platform to enhance the transparency of its marketing supply chain (*Jones, 2020*). This way, the brand can track the origins & quality of the ingredients that will be used for their products, boosting customer's trust & loyalty towards the brand. Another brand that uses blockchain is the well-known luxury brand, Louis Vuitton (LV). The brand uses Aura Consortium blockchain to reinforce the digital certificate of their diamonds. The certificate provided with each purchase, allows the purchaser to trace the diamond's origin, through how it was processed, till it is placed on the wearer (*Asher, 2024*). This approach helps to prevent counterfeit diamonds being purchased & build trust with customers, which is especially important for a luxury brand.

Due to blockchain's decentralized & transparent nature, it has offered a revolutionary approach to **content monetization & ownership**. Before blockchain, creators faced the challenges of involving intermediaries that take significant cuts from their content revenue, reducing their earnings. However, with the introduction of blockchain, creators can directly monetize their content so that they can receive their fair share of revenue. Blockchain has a secure & transparent management of content rights, allowing the creators to establish clear ownership of their work through immutable records, preventing unauthorized use or distribution of their contents. Smart contracts are able to automate the distribution of royalties, ensuring creators receive their payment in a timely manner. For instance, Audius is a decentralized music streaming platform built on the Ethereum blockchain, enabling artists to distribute music directly to the listeners, retaining control over their content while earning royalties without intermediaries (*Build My Dapp LLC, 2024*).

Challenges of Implementing Blockchain in Digital Marketing

As the adoption of blockchain is becoming more popular among industries, **scalability & transaction speed** has become a significant obstacle. Public blockchain networks tend to experience slow transaction times as they grow, which can be problematic for marketing campaigns that require fast & efficient processing of numerous transactions (*Chirag, 2024*). (*Chirag, 2024*). Transaction speed slows down due to the consensus mechanisms in the blockchain, the more transactions occur, the more congested the network becomes, resulting in delays. Current blockchain technology is struggling to quickly & efficiently handle high volumes of data.

Another challenge is the **complexity of blockchain integration** with existing marketing platforms & systems. Substantial changes to infrastructure are often involved, which can be costly & time-consuming. Ensuring the blockchain is compatible with current technologies can pose a big challenge. Additionally, blockchain technology is rapidly evolving, making it more complex as it requires one to pay constant attention to the blockchain infrastructure's latest developments. Businesses that plan to adopt blockchain technology in marketing must plan carefully before executing the integration.

[640 Words]

Propose the solution(s) for your chosen topic. [20marks]

Justify your proposed solution(s) for your chosen topic from social, legal, architecture and market perspectives.

Group Work

Social Perspective

The anonymity provided by blockchain technology has definitely helped the users to have enhanced privacy & increased security by protecting their personal information & reducing the risk of identity theft. However, it also introduced a significant social challenge. Its pseudonymous nature allows users to perform interactions without letting people know their identity, which includes committing crime while remaining unknown, making it complicated for crime tracking.

Arkham Intelligence can be used in order to cope with the pseudonymous nature of blockchain. It is an on-chain analytic platform that provides a suite of tools to obtain more detailed information available on the supported blockchain, mainly focusing on transaction data. This enables the traders to make better decisions with the obtained intelligence before investments.

Arkham Intelligence utilizes advanced software algorithms to bridge the gap between analysts. Firstly, it will collect data that might or might not be linked to real-world identities, which include pseudonymous addresses, transaction histories, & specifics of smart contract codes. After that, the collected data will be turned into usable data with the help of engineering expertise, data science, & machine learning. These will classify the pseudonymous data into “entities”. The platform then examines various data points & collects intel from multiple sources for identification. Machine learning will then play its part in further classification of the identified data by matching the “entities” to real-world counterparts through pattern recognition. Lastly, the platform has a dashboard that visualizes the processed data for analysis (*Sankrit, 2024*).

To further prove the authenticity of the data, Arkham Intelligence also has a market place named as “Arkham Intel Exchange”. It works similarly to a bounty board, where users place bounties to dox an address or entity. The community can attempt to provide information that can prove the bounty target is related to a real-world entity.

The Arkham Visualizer feature offers a bird’s eye view of an entity’s raw data. It provides visualization of transactions by interconnecting significant data points. This helps the users to recognize the patterns, trace the transactions, & understand the relationships among related entities. In general, it provides a holistic overview of the where the transactions’ inflows & outflows. Hence, helping the user to determine if the activities are suspicious.

[366 Words]

Legal Perspective

One of the main legal challenges that blockchain-related businesses face are the unregulated state of blockchain in most countries. Cryptocurrencies are viewed as tools to facilitate criminal activity, such as money laundering, in some circles. Therefore, many blockchain-related businesses are seeking regulation to prove their credibility (*Provasoli, 2018*). Several frameworks & guidelines approach can be provided for the businesses to understand & adhere to the legal requirements.

Know Your Customer (KYC) & Anti-Money Laundering (AML) Compliance

Both KYC & AML regulatory compliance are designed to prevent illegal activities. The measures of the regulations can ensure the blockchain-related businesses' transparency, security, & adherence to legal standards. Compliance with KYC & AML should be established within the business as the minimum requirements to ensure that every user goes through thorough identity verification & transaction monitoring. Staying updated to these regulations is also required to adapt to the rapidly changing blockchain industry (*Data Zoo, 2024*).

General Data Protection Regulation (GDPR) Compliance

Blockchain's main selling features is that it offers immutability, anonymity, & decentralized control. However, unless the personal data stored on the blockchain is truly anonymised, which is very difficult to truly achieve in practice, the storage & processing of blockchain data will need to comply with GDPR (*Simmons LLP, n.d.*). For instance, the businesses that adopted the blockchain technology should make clear about their transparent privacy policies by informing users about how their data is processed, stored, & protected as of Article 13 & 14 of GDPR.

Adhering to Market in Crypto-Assets (MiCA)

MiCA is a regulatory framework proposed by the European Union (EU) that governs crypto assets in Europe based on the best practices from EU's existing regulations & applying it to crypto assets (*Unchaine, 2024*). Adherence to MiCA provides legal clarity & protection to the crypto-assets market. It addresses issues related to misinformation, insider dealing, market manipulation, etc. (*GoMiCA, n.d.*). It also imposes strict transparency & disclosure requirements on crypto-assets by having accurate & clear communication on the products or services provided that contains warnings of the risks involved.

[329 Words]

Architectural Perspective

Blockchain interoperability is desired for the essential growth & development of blockchain technology to overcome the current communication limitations between different blockchain platforms & unlock the true potential of decentralized networks. With interoperability posing as an obstacle for further innovation of blockchain technology, there are several approaches that can serve as the solution.

Cross Chain Bridges

This is a technique that uses a separate blockchain to act as a bridge between two blockchains that facilitates data, assets, & messages exchanged between different blockchain networks without needing intermediaries. In short, this is a 3rd blockchain between the 2 blockchains and maintains cryptographically secured transactions & messages between them. Bridge token is one of the core elements of a cross chain bridge. It leverages the cross-chain messaging protocol by moving tokens between blockchain (*Chainlink, 2024*).

There are 3 types of main mechanisms:

Lock & Mint

- Involves user locking tokens in a smart contract on the source chain & minting the tokens on the destination chain
- In the reverse direction, the tokens on the destination chain are burned to unlock the original coins on the source chain

Burn & Mint

- Involves user burns tokens on the source chain
- The same native tokens are minted on the destination chain

Lock & Unlock

- Involves user locks tokens on the source chain
- Unlocking the same native token on the destination chain's liquidity pool

Notary Schemes

Notary verifies blockchain events & passes the information to the 2nd blockchain by acting as a 3rd party notary between 2 users on different blockchains. In order to achieve this, the notary should be registered on both the source & target blockchain platform. There are 2 types of notaries: a single-signature notary & a multi-signature notary.

A single-signature notary validates the transaction data & initiates a transaction on the target chain after collecting transaction data from the source chain. Multi-signature notaries on the other hand relies on the verification of a cross-chain request from the majority of the nodes. After verification, the transaction is then added to the target chain. The cross-chain transactions will only be processed & transmitted to the target if over $\frac{2}{3}$ of the notaries reach consensus & sign the transaction (*De Meijer, 2023*). One of the blockchain networks that uses a notary scheme is Bifrost Network, a public blockchain that is compatible with the Ethereum API.

[360 Words]

Market Perspective

As blockchain demand is increasing over the years, the scalability issues of popular blockchain networks, such as Bitcoin & Ethereum, are surfacing due to the limited transaction throughput, resulting in network congestion that affects the transaction speed (*TokenMinds, 2024*). The solutions proposed below can improve on the current issues.

Layer 2 Solutions

Layer 2 solution refers to the protocols operating on top of a base blockchain. It speeds up transaction speeds & enables better scalability without affecting the blockchain's security. Another aim of layer 2 solution is to reduce the gas fees, making blockchain interaction more affordable, which elevates user experiences.

The core workflow that layer 2 solution includes is off-chain processing. The processing of the transactions are done off the main chain & then batched together into a single transaction on the main chain record. This helps to reduce the workload of the primary blockchain, therefore enhancing the transaction throughput (*Build My Dapp LLC, 2024*) compared to traditional layer 1 solution. The security is also not compromised in this process due to the secondary protocols atop the main blockchain that define rules & optimize the system for performance without compromising the integrity.

One of the layer 2 solutions is Optimistic Rollups, which is designed to extend the throughput of the blockchain's base layer. It is an approach that has been used by the Ethereum network. It offers a significant processing speed improvement within Ethereum by bundling multiple off-chain transactions into large batches before submitting to Ethereum to spread fixed costs across multiple transactions, reducing the end-user's fees. The term "Optimistic" is based on the assumptions that the off-chain transactions are valid & honest. If the transactions are not calculated correctly, Optimistic Rollups will use its fraud-proving scheme to detect such cases & submit it to Ethereum. A time window, called a "challenge period", allows blockchain participants to challenge the results of the rollup transaction by computing a fraud proof to check if the transaction is executed honestly. If fraud proof succeeds, the rollup protocol will re-execute the transaction & update the state while also issuing a penalty to the sequencer of the incorrectly executed transaction. However, if the rollup batch remains unchallenged after the period, it will be deemed valid & accepted on Ethereum, usually it occurs only if all transactions are correctly executed (*Ethereum, 2024*).

[380 Words]

Terra Blockchain Security Breach (Whelan Yap Boon Hong)

As of 31 July 2024, one of the more well-known blockchain platforms, Terra, has suffered from a security breach that resulted in token theft (*Chawla, 2024*). An approximate amount of \$5M worth of tokens were compromised.

Cause of Security Breach

The attacker had taken advantage of the platform's Inter-Blockchain Communication (IBC) hook that facilitates the interoperability & data transmission between blockchains (*Haqshanas, 2024*). Cyvers Alert, a Web3 security firm, stated that the attacker exploited the platform with a reentrancy attack (*Malwa, 2024*). This attack exploits the smart contract by repeatedly triggering "timeout callback" & allowed the attacker to manipulate the contract's state. Although this vulnerability was identified & patched previously in April, the fix was unintentionally reversed in a June update, which was suspected to be not including the patch fixes on the subsequent update. Temporary measures were done as of press time to prevent similar exploits from occurring. However, the news of the breach had caused a significant impact to Astroport's ASTRO token, hosted on the Terra Network, to suffer a 60% drop in value within 24 hours following the incident.

Stakeholders Involved

Developers

- Responsible for developing the blockchain platform while ensuring the appropriate security measures are implemented
- Identifying & patch any existing vulnerabilities, continuously improving the security framework, & inform users about the breach if any happens

Investors & Users

- Uses the platform by depositing their assets & data while also has the power to demand accountability & transparency from the platform
- If breaches happen, they can withdraw their assets & data from the platform & spread the information to other users, or seek for compensation if losses occur while pressuring the platform to improve their security measures

Regulators

- Creating guidelines & standards and enforce regulation compliance to protect users & integrity of the blockchain network
- When breaches happen, they are responsible for investigating the incident & develop stricter security standard for the blockchain platform

Ethical Considerations

When the security breach occurred, Terra halted its operation until patches were done. The platform has done a good job in informing all the stakeholders about the breach & what measures were taken to address the incident. This justifies their action that can keep the company's long-term self-interest in the perspective of *ethical egoism*.

When the security breach happens, Terra immediately stops its operation & addresses the issue to keep the investors & users informed so that it can minimize the negative impact on both of the parties. Terra also stated they will keep all the stakeholders updated on the issue

until it is resolved to improve the overall well-being, which fits “*Utilitarianism*”, specifically “*Preference Utilitarianism*” & “*Negative Utilitarianism*” that aims to produce the most favourable consequences in terms of happiness & reduce negative consequences.

“*Kantianism*” emphasizes on ethical morals, which Terra portrayed by taking full responsibility for the security breach instead of shifting the blame to the IBC module or intentionally avoiding responding to the incident. Their actions respect the stakeholders by showing them honesty & transparency, which will ensure continuous trust & cooperation between the two parties.

Beliefs & Values

I firmly believe that blockchain is an incredible technology & holds a lot of potential for revolutionizing the future market of various industries despite the Terra security incident. The decentralization & transparency nature offered by the blockchain allows users to view transactions & manage data openly, letting the user know that nothing is hidden from them. This transparency builds trust between the users & the blockchain platform. The blockchain technology currently has the ability & is already transforming the industries workflow. For instance, in supply chain management of an organization, blockchain plays the role of tracking the goods as well as its sources, ensuring the authenticity of the goods. Customers can also view all relevant product information, from the source to the point of sale, providing the customers a sense of relief & confidence before purchasing the goods.

I also believe that the developer & operators of the blockchain platform must take responsibility & accountability for their actions or any incidents that occur, just like Terra. Ensuring transparent communication & promptly addressing any issues regarding the security incident instead of staying silent shows that the platform is well aware of the incident & is committed to maintain user trust & platform security. This allows the investors & users to make informed decisions whether to continue supporting the platform, therefore minimizing their losses. In order to ensure the long-term success of the blockchain technology, this proactive approach helps in fostering a sense of security & reliability towards the blockchain. It also sets a good example or standard in the industry, encouraging other blockchain platforms to do the same to demonstrate accountability & transparency. By doing so, people will place more trust & confidence in the blockchain technology, allowing it to evolve & thrive in various sectors.

Attitudes & Assumptions

As technology advances quickly nowadays, it is no doubt that blockchain technology & its security will be evolving continuously. However, it may also be a great challenge because threat actors can also develop new advanced attack techniques to exploit the vulnerabilities at that time, making it complex to completely cover every security aspect & potential loopholes within the technology as time advances. Let's assume that even if blockchain technology is able to cover all technical vulnerabilities, it's hard to say that it is completely invulnerable due to the existence of human error, which is an unstable variable in security assurance. According to the report made by Cybersecurity Insider, 74% of the companies are moderately vulnerable to insider threats & is most caused by employee's negligence (*Laborde, 2024*). Individuals with poor security awareness can be exploited with social engineering tactics that tackle human vulnerabilities, allowing the attack to take place & succeed internally, no matter how sophisticated the security measures are. Taking Terra as an example, they reversed the patch that could have prevented the incident from happening.

[948 Words]

Mixin Network Security Breach (Pang Jin Siang)

Mixin Network is a Hong Kong-based platform that operates a peer-to-peer transactional network for digital assets founded in 2017. Mixin Network experienced a hack attack on September 23, 2023. The main assets targeted in this attack were ETH, BTC, and USDT-ERC20, and other coins also suffered losses.

Cause of Security Breach

The Mixin Network attack was primarily caused by a leak in the cloud service provider's database. This breach resulted in unauthorized access to the network's hot wallets. One important weakness that was taken advantage of in this attack was the centralized nature of the database that Mixin Network used.

Stakeholders Involved

- **Mixin Network Users**
These are individuals and entities who trusted Mixin Network with their assets. They are directly affected by the breach, as they have potentially lost significant amounts of money.
- **Mixin Network**
The company itself is a central stakeholder, responsible for ensuring the security of its platform. It holds significant power over how it responds to the breach, including decisions about compensation, transparency, and future security measures.
- **Cloud Service Provider**
This entity is responsible for the database that was compromised. Their ethical responsibility lies in ensuring the security of the services they provide to clients like Mixin Network. However, their power to act is constrained by the terms of the service agreement with Mixin.
- **Regulator**
Although not directly involved in the breach, regulators have an indirect stake in ensuring that blockchain platforms operate within a framework that protects consumers. Their power lies in the ability to enforce regulations and potentially hold Mixin Network accountable.

Ethics Philosophies

Kantianism

Kantian ethics focuses on the idea that actions must be guided by universal moral principles, such as duty, honesty, and respect for individuals. In the case of the Mixin Network breach, Kantianism would stress the importance of the company's duty to protect its users' assets. Mixin Network should have implemented stringent security measures, not just to avoid financial loss, but because it is the right thing to do according to a universal moral law. The breach suggests a failure to fulfil this duty, raising ethical concerns about whether the company treated its users with the respect they deserve as autonomous individuals.

Utilitarianism

Utilitarianism evaluates the morality of actions based on their outcomes, aiming to maximize overall happiness or minimize suffering. The ethical consideration here revolves around the significant harm caused to Mixin Network users due to the breach. If the company's decisions led to a loss of \$200 million and widespread distress among its users, then from a utilitarian

perspective, those decisions were ethically wrong because they resulted in more harm than good. Mixin Network's failure to prevent the breach indicates a neglect of its ethical obligation to maximize the well-being of its users.

Ethical Egoism

From this perspective, when the security breach occurred, Mixin Network temporarily suspended their deposit and withdrawal services. Mixin also announced the incident and action taken to address it on x.com (Twitter) to the stakeholders. This justifies their action that can keep the company's long-term self-interest in the perspective of *ethical egoism*.

Belief

I believe that blockchain technology offers enhanced security and integrity for digital transactions. The use of cryptography and consensus mechanisms is seen as a way to protect data from unauthorized access and tampering. This belief is underpinned by the idea that blockchain's immutable nature ensures that once data is recorded, it cannot be altered without detection, thus preserving the integrity of the information.

Value

The value of security is important in technology. In the digital age, the protection of user's assets and data is the most important. Platforms such as Mixin Network must prioritize security at all stages of their operations. This value is based on the concept that users' trust is a platform's most important asset, which must be acquired and maintained through strong security measures.

Attitudes

Regarding the Mixin Network breach I am largely concerned. While knowing that no system can be completely secure, the fact remains that there was such a gaping hole in a platform where users entrusted their economic lives with. The event has made me become more suspicious of any claims made by blockchain platforms regarding its safety.

Assumptions

I do assume that blockchain technology is highly reliable due to its decentralized nature and the use of consensus mechanisms like proof-of-work or proof-of-stake. This assumption leads me to believe that blockchain networks are less prone to downtime or failure compared to centralized systems. However, this assumption might overlook potential vulnerabilities, such as network congestion or attacks on smaller, less secure blockchains.

[755 Words]

Binance Cryptocurrency Theft Incident (Lee Kong Hang)

On 4th October 2022, Binance Holdings Ltd, the largest company that allows users to exchange cryptocurrencies (*Binance, n.d.*), had suffered from a cyberattack that resulted in token theft. An estimated amount of 2 million Binance Coins (BNB) were stolen, which can be exchanged for over \$570 million (*Firch, 2024*). This attack has highlighted the weakness in decentralized finance (De-Fi), where there are no intermediaries to audit & verify the transactions (*Livni, 2022*). As a result, they notified the users on their social media, announcing that they had halted their operation temporarily.

Cause of Cyber Attack

The Binance Smart Chain Token Hub cross-chain bridge, a protocol that enables the transfer of tokens & other assets between blockchain networks, is exploited by the hacker (*Barchat, 2024*). The hacker created & withdrew 2 million BNB by exploiting the bug within the smart contract (*George, 2024*), allowing the acceptance of forged fake proof messages. After successfully withdrawing the tokens, the hacker started to transfer them to other liquidity pools so that it can be converted into other assets (*Firch, 2024*).

Stakeholders Involved

- ***Binance***
As the company that suffered from the losses, it suffered from financial & reputational damage. The public also raised their concerns about its ability to maintain the security of the platform & how the incident will be resolved along with their way to resolve the incident.
- ***Binance Coin Holders (Investors & Users)***
The investors & users that hold the Binance cryptocurrency may face the consequences of the value drop of Binance Coin, which may impact them financially. This created questions & trust issues between them & Binance.
- ***Binance Smart Chain Developers***
The incident that resulted in the loss of around \$570 million had pressured them to fix & resolve the underlying infrastructure of the vulnerable smart contract code. Activities on the Binance platform are temporarily halted to allow the developers to focus on solving the issues, which in turn affecting their project timelines.
- ***Regulatory Bodies***
The regulators may have noticed this incident as a major issue & may scrutinize Binance's operation & other cryptocurrencies platforms to prevent the similar incident from happening. Tighter regulations & compliance requirements may be enforced.

Ethical Considerations

Divine Command Theory

Divine Command Theory is an ethical theory that asserts that moral values and duties are derived from the commands or will of a divine being or God. According to the values of most religions, the act of stealing or theft is considered unethical, which can be further proved by the 8th commandment of God "You shall not steal". The act of token theft done by the hacker violates the religious commandment, therefore it is morally wrong. On the other hand, Binance's act of protecting users & trying to recover the stolen token can be viewed as upholding their justice while being morally right.

Ethical Egoism

Ethical egoism upholds self-interest as the guide of morality. In the point-of-view of Binance, their act of protecting their reputation & minimizing losses can be justified by securing the platform's security while also letting their stakeholders & users regarding their approach on the attack.

Kantianism

From a *Kantianism* perspective, the hacker's action is unethical due to the concept of Kantianism that judges moral value by looking at the action done, regardless of the outcome. What the hacker has done clearly violates the moral value of honesty, which is unethical, not to mention that the outcome is also significant, in a bad way. As for Binance, they too can be considered being unethical due to failure of fulfilling their promises to protect its users & maintain the integrity of the platform.

Beliefs & Values

Based on the incident, I believe that Binance actually places the platform's security at a high place by safeguarding the assets against various cyberattacks to maintain the stakeholders' trusts & confidence. Although their assets were compromised, they are actively trying to resolve the issue while also being transparent about the situation. They are also honest about their failure to detect the vulnerability & causing the incident to happen. I also believe that the hacker will be held accountable for his or her unethical actions.

Attitudes & Assumptions

As time goes on, I believe that Binance's security infrastructure will be progressively advanced. However, gaining back the public's complete trust will be difficult as the incident mentioned is not the first time that Binance has suffered from losses due to cyber attacks. There was a prior case of 7000 bitcoins being stolen in 2019, that cost the company almost \$40 million while the funds were also not found nor recovered. As for the recovery of lost funds in the 2022 case, the public might also be skeptical about it. If the same incident reoccurs, the stakeholders might choose to give up on investing in the Binance platform or demand for compensation.

[790 Words]

Ronin Network Hack (Lim Ying Thong)

A significant security breach occurred in March 2022 on the Ronin Network, a blockchain that powers the well-known game Axie Infinity. As a result, hackers were able to take over \$625 million worth of Bitcoin (*Antoniuk, 2024*). Through the use of flaws in the validator nodes of the network, the hackers were able to validate illegal transactions on five out of nine validators.

Cause of Security Breach

The primary cause of the Ronin Network breach was the exploitation of a flaw in the network's validator nodes. The attackers were able to authorize transactions that weren't authorized by control over five of the nine validators (*roninchain.com, 2022*). In addition, a platform that operates on the Ronin Network decided to loosen its security measures because of the overwhelming increase in users caused by the quick expansion of Axie Infinity (*TIDY, 2022*). The validator system's vulnerability was also accidentally established by a bridge upgrade that was carried out through the governance process which made the network's defenses even weaker and made attackers facilitate the penetration and execution of the breach (*Toulas, 2024*). Due to their appreciation, the stolen assets serve as a reminder of the inherent hazards connected to decentralized finance and cryptocurrencies. A \$625 million loss of bitcoin was the eventual consequence of the network being left vulnerable by a lack of timely upgrades and security patches.

Stakeholders Involved

- **Developers and Validators**
The developers and validators were responsible for maintaining the security and operation of the Ronin Network. They had to fix the damage, inform users of the situation, and put in place more robust security measures to fend off such assaults after the occurrence.
- **Investors and Users**
Investors and users relied on the Ronin Network to securely manage their assets. The breach immediately impacted them causing large financial losses. In order to safeguard their investments, they had to put pressure on the network to pay them, provide transparency, and advance improved security procedures.
- **Regulators**
Regulators were responsible for ensuring that the Ronin Network complied with security standards and protecting users from potential risks. Following the breach, they investigated the incident, implemented tighter regulations, and campaigned for more robust regulatory frameworks within the blockchain sector in order to stop such occurrences in the future.

Ethical Considerations

The Ronin Network hack highlights key ethical issues related to balancing between security and rapid development. The creators owed it to their users to provide them with comprehensive safety according to *Kantian* ethics. They violated this responsibility by putting rapid expansion ahead of user trust. This choice is similarly criticized by *utilitarianism* since it went against the objective of optimizing well-being generally and caused significant harm. Comprehensive safety would have been preferred by *negative utilitarianism* to prevent suffering, even at the expense of slower economic progress.

Moreover, the *Social Contract Theory* proposes an implicit agreement in which users believe developers in return for developers' maintenance of platform integrity. Although developers addressed the issues and compensated users, the initial lack of security breached this contract and ultimately weakened user confidence.

In addition, the developers' response corresponds with *Ethical Egoism* as they acted in their long-term self-interest by addressing the breach and compensating users to restore trust and retain their user base. However, *Kantian ethics* reminds us that the legal responsibility to protect users should have been upheld from the start, and reactive efforts cannot fully compensate for this fundamental ethical failure. This situation underscores the importance of proactive ethical behavior to ensure long-term security and sustain platform confidence.

Beliefs & Values

The fundamental principles and ideals that should guide the creation and operation of blockchain platforms are highlighted by the Ronin Network hack. The core principle of blockchain technology is that the highest level of security must be implemented for user assets. However, the Ronin Network's creators seem to have compromised these principles in the name of speed and scalability which resulted in a devastating breach. The event brings to light the conflict between corporate goals and the core principles of security, integrity, and user trust. The network's image has suffered and there has been a sizable financial loss as evidence of the dire consequences that can arise from compromising these ideals.

The creators restored the fundamental principles that should have been maintained from the beginning by compensating users and strengthening security in reaction to the compromise. Nevertheless, the lost confidence cannot be completely restored by this reactive strategy. The hack serves as a warning that, despite commercial demands, principles like security, responsibility, and transparency must always come first. Understanding these principles continuously is not only an issue of ethical responsibility but also essential to any blockchain platform's reputation and long-term survival.

Attitudes & Assumptions

The Ronin Network breach reveals improper attitudes and assumptions that caused the security compromise. The original overconfidence in the network's security infrastructure was a crucial attitude. Security standards were loosened as a result of this overconfidence which caused the belief that the network could support growing user traffic without creating serious hazards. This was a serious mistake on the part of the developers, who thought the security mechanisms in place were enough. Significant contributing elements to the breach were the complacent attitude and the belief that the network was inherently secure.

The incident challenges the assumption that decentralized networks are inherently secure and highlights the dangers of not continuously reassessing and updating security measures. The hack shows that hazards rise along with networks' expansion and evolution, requiring continuous attentiveness and proactive management. It offers significant lessons such as the need to constantly verify security assumptions and the fact that overconfidence in current systems can result in serious flaws. In the future, it is essential to adopt a mindset of continuous improvement and caution to ensure that security remains a top priority in the management of blockchain platforms.

[943 Words]

Poly Network Hack (Ong En Ting)

In August 2021, the Poly Network, a well-known decentralized finance (DeFi) platform experienced a major security breach that resulted in the theft of over \$600 million worth of various cryptocurrencies. This incident raises significant ethical questions surrounding cybersecurity, user trust and the responsibilities of various stakeholders in blockchain technology (*Shen, 2021*).

Cause of Security Breach

The Poly Network hack of August 2021, which resulted in the theft of over \$600 million worth of cryptocurrencies, exemplifies the vulnerabilities inherent in decentralized finance (DeFi) platforms. The breach was primarily caused by a flaw in the smart contract code used by Poly Network, which facilitated the transfer of assets across different blockchains. Specifically, the vulnerability arose from improper handling of permissions within the smart contracts. This flaw allowed the attackers to manipulate the system, enabling them to execute unauthorized transactions without the necessary validations. By exploiting this oversight, the hackers were able to unlock tokens on various blockchains, including Ethereum, Binance Smart Chain and Polygon without locking the corresponding amounts on the source blockchain. The attack highlighted the critical need for robust security measures and thorough audits of smart contracts, as the decentralized nature of blockchain technology can sometimes lead to insufficient oversight and risk management. Furthermore, the incident underscored the importance of implementing stringent access controls and ensuring that smart contract interactions are meticulously validated to prevent similar exploits in the future (*Network, 2023*).

Key stakeholders in this incident included:

- ***Poly Network:***
As the platform's operator, Poly Network had the responsibility to secure user funds and maintain trust in their platform. After the breach, they attempted to negotiate with the hacker, offering a bounty and a role as a security advisor, which led to the eventual recovery of most of the stolen assets.
- ***Users whose funds were stolen:***
Users directly affected by the hack faced significant financial loss and a severe erosion of trust in the platform. Many users experienced stress and uncertainty, underscoring the personal impact of cybersecurity failures.
- ***The Hacker (later referred to as "Mr. White Hat")***
The individual behind the hack, who later claimed to have acted to expose vulnerabilities rather than for personal gain, sparked significant debate regarding ethical behavior. Their decision to return the stolen funds and disclose the vulnerabilities can be viewed as a complex blend of ethical considerations.
- ***Cryptocurrency Community and Regulatory Bodies:***
Regulatory bodies and the cryptocurrency community play crucial roles in shaping security standards and practices, emphasizing the collective responsibility to enhance security in the DeFi ecosystem (*Russon, 2021*).

Ethical Considerations

The ethical considerations surrounding the Poly Network hack can be analyzed through various frameworks. From a *Utilitarian* perspective, while the initial act caused distress and financial loss for users, the hacker's decision to return the funds can be seen as a positive outcome that contributes to the greater good. This perspective highlights the complexity of evaluating actions based solely on their consequences. In contrast, *Kantianism* ethics emphasizes the importance of duty and moral principles. The hacker's theft violated the principles of honesty and respect for property, rendering the act ethically indefensible, regardless of the subsequent return of the assets. According to Kantianism, the act of stealing, even with good intentions, is inherently wrong. Finally, *social contract theory* suggests that all parties involved have an implicit agreement to uphold certain ethical standards. Poly Network's failure to secure user funds and the hacker's breach of trust both represent violations of this social contract, underscoring the need for accountability and ethical conduct in the digital finance space (*MCopper, 2019*).

Beliefs & Values

Reflecting on the beliefs and values revealed by this incident, I can deeply recognize the centrality of trust, security and ethical responsibility in the cryptocurrency ecosystem. Users expect their assets to be secure, necessitating robust security measures and continuous vigilance. The breach exposed significant security flaws and underscored the need for transparent communication to restore trust. Additionally, the ethical implications of the hacker's actions, despite returning the stolen funds, demonstrate the importance of ethical behavior from all stakeholders to ensure a trustworthy and reliable digital finance environment (*The420.in, 2021*).

This incident has also highlighted the necessity for ongoing education within the cryptocurrency community about security practices and the importance of ethical hacking. As the DeFi space continues to evolve, fostering a culture of transparency and accountability will be essential to maintaining user trust and protecting assets.

Attitudes & Assumptions

The attitudes and assumptions regarding the Poly Network hack have shifted significantly in my perspective. Initially, I viewed the hacker as a criminal for orchestrating one of the largest thefts in cryptocurrency history, stealing over \$600 million. However, as the story unfolded and the hacker returned the funds while claiming to have acted to expose vulnerabilities in the system, my view began to change.

This transformation in perception illustrates the complexity of motivations behind such actions. I now recognize that ethical behavior can exist in shades of grey rather than being strictly black and white. The incident highlights the ongoing risks in the decentralized finance (DeFi) space and reinforces the importance of prioritizing ethical practices and enhancing security measures to protect users in the future.

[840 Words]

References

1. Mastering Blockchain. (n.d.). Retrieved from https://books.google.com.my/books?hl=en&lr=&id=urkrDwAAQBAJ&oi=fnd&pg=PP1&dq=blockchain&ots=Ix9o8l9uXP&sig=sve49wVML3Qw1SL3RJbackK4frA&redir_esc=y#v=onepage&q=blockchain&f=false
2. Blockchain in Cryptocurrency: Beginner Guide and Career Outlook. (n.d.). Retrieved from <https://www.coursera.org/articles/blockchain-cryptocurrency>
3. Mindmajix. (n.d.). ▷ Components of Blockchain - MindMjaix. Retrieved from <https://mindmajix.com/components-of-blockchain#components>
4. Shoemaker, P. (2024). Key Components of a Blockchain Network. Retrieved from https://www.identity.com/key-components-of-a-blockchain-network/#Main_Components_of_a_Blockchain_Network
5. Blockchain stakeholder Understanding the Role of Blockchain Stakeholders in Decentralized Networks. (n.d.). Retrieved from <https://fastercapital.com/content/Blockchain-stakeholder-Understanding-the-Role-of-Blockchain-Stakeholders-in-Decentralized-Networks.html#:~:text=Introduction%20to%20Blockchain-1,activities%20within%20the%20blockchain%20network>
6. Kshetri, N. (2021). Blockchain technology for improving transparency and citizen's trust. In Advances in intelligent systems and computing. https://doi.org/10.1007/978-3-030-73100-7_52
7. Kisawuzi, J. K. (2023, December 20). Revolutionizing Cross-Border Payments. <https://www.linkedin.com/pulse/blockchain-revolutionizing-cross-border-payments-afrikan-kisawuzi-tokaf/>
8. Dulani Woods. (2023, January 12). Cryptocurrency and Blockchain Needs for Law Enforcement. https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR108-17/RAND_RRA108-17.pdf
9. Team, I. (2024, April 23). What was Mt. Gox? Definition, history, collapse, and future. <https://www.investopedia.com/terms/m/mt-gox.asp>
10. FATF, n.d., 2024. Virtual assets. <https://www.fatf-gafi.org/en/publications/Virtualassets/Virtual-assets.html>
11. Ma, A., & Wales, E. (n.d.). EMERGING LEGAL ISSUES IN BLOCKCHAIN FOR CONSTRUCTION SUPPLY CHAINS. <https://www.open-access.bcu.ac.uk/9942/1/DC1001%2C%20Ma%2C%20Blockchain%20Legal.pdf>
12. IMF, (2023, March 22). Anti-Money laundering and combating the financing of terrorism. <https://www.imf.org/en/Topics/Financial-Integrity/amlcft>

13. Blockchain in Law | Real World Blockchain Use Cases. (n.d.). Consensys.
<https://consensys.io/blockchain-use-cases/law>
14. Simmons. (n.d.). GDPR and Blockchain.
<https://www.simmons-simmons.com/en/publications/ck0ab739h6lqx0b94c446zltz/130918-gdpr-and-blockchain>
15. Llc, B. M. D. (2024, March 24). Blockchain in Real Estate.
<https://www.linkedin.com/pulse/blockchain-real-estate-transforming-property-transactions-vvhxf/>
16. FATF. (n.d.). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Retrieved from
<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>
17. <https://consensys.io/blockchain-use-cases/law>
18. Baftijari, A. B., & Nakov, L. (2024). The Architecture of Blockchain Technology and Beyond. In *www.intechopen.com*. IntechOpen.
<https://www.intechopen.com/online-first/1184120>
19. Hayes, A. (2023, December 15). *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*. Investopedia; Dotdash Meredith.
<https://www.investopedia.com/terms/b/blockchain.asp>
20. IBM. (n.d.). *Benefits of blockchain - IBM Blockchain | IBM*. Wwww.ibm.com.
<https://www.ibm.com/topics/benefits-of-blockchain#:~:text=Because%20blockchain%20uses%20a%20distributed>
21. Medicalchain. (2022). *Home*. Medicalchain.
<https://medicalchain.com/en/#:~:text=A%20Smart%20Medical%20Ecosystem&text=Fragmented%2C%20siloed%20patient%20records%20create>
22. Reportlinker. (n.d.). *The global blockchain market size is expected to grow from USD 3.0 billion in 2020 to USD 39.7 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 67.3%*. Wwww.prnewswire.com.
<https://www.prnewswire.com/news-releases/the-global-blockchain-market-size-is-expected-to-grow-from-usd-3-0-billion-in-2020-to-usd-39-7-billion-by-2025--at-a-compound-annual-growth-rate-cagr-of-67-3-301058443.html>
23. Build My Dapp LLC. (2024, April 25). *The Limitations and Challenges of Blockchain Technology*. Wwww.linkedin.com.
<https://www.linkedin.com/pulse/limitations-challenges-blockchain-technology-build-my-dapp-iduzf>
24. MCopper. (2019, January 29). Five Workable Ethical Theories - MCopper - Medium. Medium; Medium.
<https://medium.com/@mccccc/five-workable-ethical-theories-a8bfa0a49f37#:~:text=Kantianism%2C%20rule%20utilitarianism%20and%20social>

25. Network, P. (2023, November 20). The Poly Network Exploit Analysis. Medium.
<https://polynetwork.medium.com/the-poly-network-exploit-analysis-b0a77aff6078>
26. Russon, M.-A. (2021, August 11). Cryptocurrency heist hacker returns \$260m in funds. Bbc.com; BBC News. <https://www.bbc.com/news/business-58180692>
27. Shen, E. G. and M. (2021, August 10). Cross-Chain DeFi Site Poly Network Hacked; Hundreds of Millions Potentially Lost. Wwww.coindesk.com.
<https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/>
28. The420.in. (2021, August 24). Hacker Returns More Than \$600 Million Stolen From Poly Network In Biggest Cryptocurrency Heist. The420.In.
<https://www.the420.in/hacker-returns-more-than-600-million-stolen-from-poly-network-in-biggest-cryptocurrency-heist/>
29. Bhardwaj, C. (2024). The Rise of Blockchain in Marketing: Benefits & Challenges. Retrieved from
<https://appinventiv.com/blog/blockchain-marketing/#:~:text=Blockchain%20technology%20is%20revolutionizing%20digital,security%20and%20privacy%20for%20users>
30. Khatri, Y. (2021). PepsiCo Blockchain Trial Brings 28% Boost in Supply Chain Efficiency. Retrieved from
<https://www.coindesk.com/markets/2019/05/06/pepsico-blockchain-trial-brings-28-boost-in-supply-chain-efficiency/>
31. Andrea Durkin 02 December 2016, Donald J. Boudreaux 04 May 2017, & Anne Kim 18 May 2017. (2019). Blockchain for tracking trade. Retrieved from
<https://www.hinrichfoundation.com/research/tradevistas/tech/blockchain-tracking-trade/#:~:text=Using%20blockchain%20technologies%20to%20track,information%20about%20globally%20produced%20goods>
32. Jones, M. (2020). Nestlé – why the world’s biggest food company is using blockchain. Retrieved from
<https://techhq.com/2020/07/nestle-why-the-worlds-biggest-food-company-uses-blockchain/>
33. LLC, B. M. D. (2024). Blockchain in the Entertainment Industry: NFTs, Royalties, and Content Ownership. Retrieved from
<https://www.linkedin.com/pulse/blockchain-entertainment-industry-nfts-royalties-content-0dvff#:~:text=Audius%3A%20A%20decentralized%20music%20streaming,and%20earn%20royalties%20without%20intermediaries>
34. Asher, J. (2024). Louis Vuitton Uses Blockchain Tech to Trace Natural Diamonds. Retrieved from
<https://www.naturaldiamonds.com/responsible/louis-vuitton-custom-cut-natural-diamond-blockchain/#:~:text=A%20digital%20certificate%20will%20let%20you%20follow%20your%20natural%20diamond's%20journey.&text=In%202022%2C%20Louis%20Vuitton%20made,diamond%2C%20the%20LV%20Monogram%20Star>
35. d’Anconia, F. (2017). Georgia Becomes First Country to Register Property on Blockchain. Retrieved from

<https://cointelegraph.com/news/georgia-becomes-first-country-to-register-property-on-blockchain>

36. K, S. (2024). What Is Arkham Intelligence and How to Use It? Retrieved from <https://www.coingecko.com/learn/what-is-arkham-intelligence-crypto>
37. What Is A Cross Chain Bridge?: Chainlink. (n.d.). Retrieved from <https://chain.link/education-hub/cross-chain-bridge>
38. Finextra. (2023). Blockchain interoperability solutions and challenges: Where are we now? Retrieved from <https://www.finextra.com/blogposting/25112/blockchain-interoperability-solutions-and-challenges-where-are-we-now>
39. (N.d.). Retrieved from <https://tokenminds.co/blog/blockchain-development/layer-2-solutions>
40. LLC, B. M. D. (2024). Addressing Scalability Challenges in Blockchain: Scalability Solutions and Their Implications. Retrieved from <https://www.linkedin.com/pulse/addressing-scalability-challenges-blockchain-solutions-implications-8ionf#:~:text=Scalability%20Solutions,-To%20address%20scalability&text=Sharding%3A%20Sharding%20involves%20partitioning%20the,can%20significantly%20increase%20transaction%20throughput>
41. Anthony Provasoli Deputy Head of Financial Services. (2024). Regulation of blockchain business – a jurisdiction comparison. Retrieved from <https://www.gibraltarlaw.com/insights/post/102il2r/regulation-of-blockchain-business-a-jurisdiction-comparison/>
42. The Critical Role of KYC & AML Compliance in Cryptocurrency. (n.d.). Retrieved from <https://www.datazoo.com/the-critical-role-of-kyc-and-aml-compliance-in-cryptocurrency#:~:text=Both%20KYC%20and%20AML%20are,and%20adherence%20to%20legal%20standards>
43. Terra Blockchain Suffers Security Breach, With \$5.28M in Estimated Losses. (2024). Retrieved from <https://cryptonews.com/news/terra-blockchain-suffers-security-breach/>
44. Malwa, S. (2024). Terra Blockchain Restarts After \$4M Exploit. Retrieved from <https://www.coindesk.com/tech/2024/07/31/terra-blockchain-restarts-after-4m-exploit/#:~:text=Terra%20blockchain%20halted%20operations%20on,reappeared%20in%20a%20June%20upgrade>
45. Laborde, S. (2024). 31 Insider Threat Statistics You Need to Know in 2023. Retrieved from <https://techreport.com/statistics/cybersecurity/insider-threat-statistics/#:~:text=According%20to%20a%20Cybersecurity%20Insiders,were%20caused%20by%20employee%20negligence>
46. Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins. (n.d.). Retrieved from <https://www.binance.com/en>

47. Firch, J. (2024). \$570M Binance Hack: What Happened & Who Is Responsible? Retrieved from <https://purplesec.us/breach-report/binance-coin-hack/>
48. What are cross-chain bridges? How interoperable crypto transfers work. (n.d.). Retrieved from <https://www.moonpay.com/learn/blockchain/what-are-cross-chain-bridges>
49. George, K. (n.d.). The Largest Cryptocurrency Hacks So Far. Retrieved from <https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/>
50. Livni, E. (2022). Binance Blockchain Hit by \$570 Million Hack, Exposing Crypto Vulnerabilities. Retrieved from <https://www.nytimes.com/2022/10/07/business/binance-hack.html>
51. d, U. (2024). What Is MiCA And What Does It Mean for Crypto Users in Europe? Retrieved from <https://www.coindesk.com/learn/what-is-mica-and-what-does-it-mean-for-crypto-users-in-europe/>
52. Mixin 923 Hacker Incident Disclosure and Progress. (2024). Retrieved from <https://mixin.network/923/>
53. Sarkar, A. (2023). Mixin Network hack drains \$200M from mainnet assets. Retrieved from <https://cointelegraph.com/news/mixin-network-hack-200-m-crypto-assets>
54. Reynolds, S. (2023). Mixin Network Losses Nearly \$200M in Hack. Retrieved from <https://www.coindesk.com/tech/2023/09/25/mixin-network-losses-nearly-200m-in-hack/>
55. ImmuneBytes, & ImmuneBytes. (2023). Mixin Network Security Breach-Sep 23, 2023-Detailed Analysis. Retrieved from <https://www.immunebytes.com/blog/mixin-network-security-breach-sep-23-2023-detailed-analysis/>
56. Vishal Chawla. (2024). Attacker exploits IBC hooks vulnerability to steal tokens on Terra blockchain/ Retrieved from <https://www.theblock.co/post/308440/attacker-exploits-ibc-hooks-vulnerability-to-steal-tokens-on-terra-blockchain>
57. Springer, Cham. (2020). SoK: Layer-Two Blockchain Protocols. Retrieved from <https://eprint.iacr.org/2019/360.pdf>
58. Antoniuk, D. (2024, August 9). Hackers return \$12 million taken during Ronin network breach. The Record. Retrieved from <https://therecord.media/hackers-return-12-million-taken-from-ronin-network>
59. roninchain.com. (2022). Ronin Blog | Community Alert: Ronin Validators Compromised. Roninchain.com. <https://roninchain.com/blog/posts/community-alert-ronin-validators-6513cc78a5edc1001b03c366>

60. TIDY, J. (2022, March 30). Ronin Network: What a \$600m hack says about the state of crypto. BBC News. <https://www.bbc.com/news/technology-60933174>
61. Toulas, B. (2024, August 7). Ronin Network hacked, \$12 million returned by “white hat” hackers. BleepingComputer; BleepingComputer. <https://www.bleepingcomputer.com/news/security/ronin-network-hacked-12-million-returned-by-white-hat-hackers/>