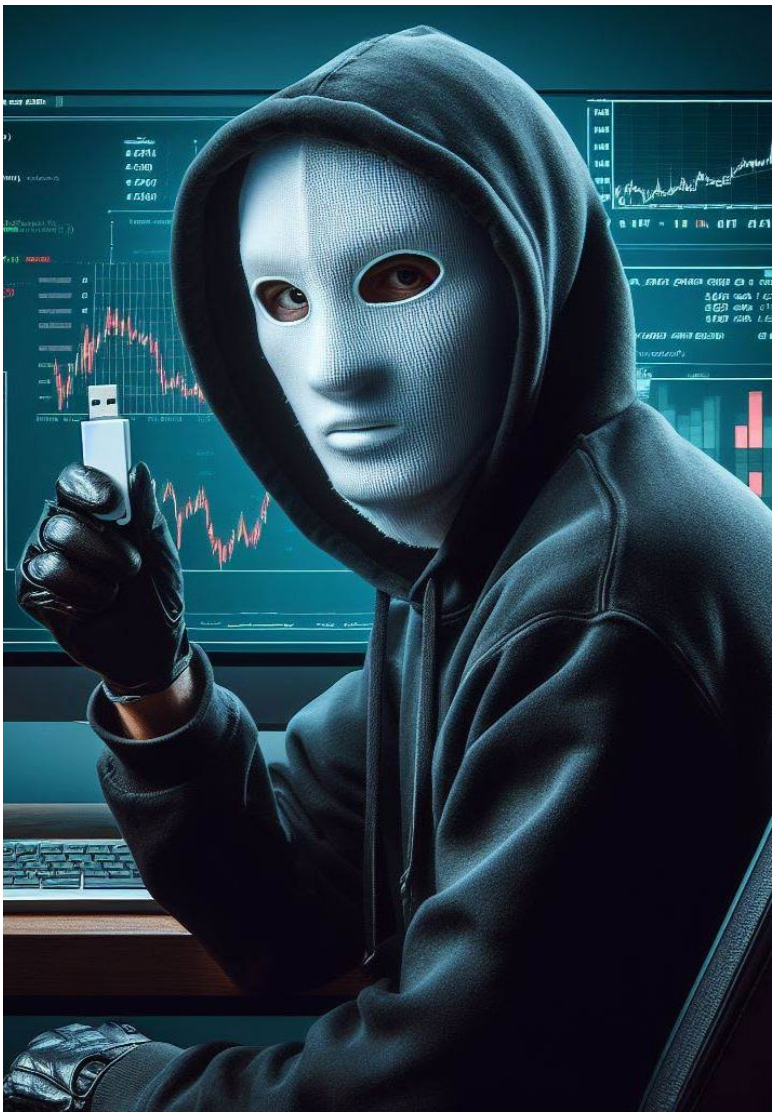


Assignment 3 (Group Set 3)

COMPUTING TECHNOLOGY INNOVATION PROJECT

Yiannis Kyritsis (103980370) | Hridoy Ahmed (103798793) | Hiyoshi Woods (103392438)

Incident Overview

On the 1st of November 2022, a significant security incident occurred involving Deribit Exchange. Deribit Exchange. Deribit Exchange is a large cryptocurrency exchange and is the largest crypto options exchange by volume and open interest. This security incident was a breach, and resulted in unauthorised access and subsequent withdraws from Deribit's hot wallets, raising alarms around the crypto community, and many Deribit users.

The initial unauthorised transaction, which marks the beginning of the breach, was detected on November 1, 2022, at approximately 00:27:23 (UTC). This was the moment that a substantial amount of Ethereum was transferred from Deribit's wallet to an external address, which was later identified as belonging to one of the hackers.

The main entities involved were the following:

Deribit Exchange:

ETH Address: 0x58F56615180A8eeA4c462235D9e215F72484B4A3

BTC Address: Too many to list, they had hundreds of affected BTC addresses.

They were the victim of the cyber-attack and are a popular exchange platform that provides trading services for various digital assets and cryptocurrencies.

Hacker 1:

ETH Address: 0xb0606F433496BF66338b8AD6b6d51fC4D84A44CD

BTC Address: bc1q2dequzmk5vk8nmmrata8nq4y0zgqn4vc0n2h8y

This was one of the suspected entities behind the breach. This address was also the recipient of the first unauthorised Ethereum transfer from Deribit's wallet and was also involved in significant Bitcoin transactions.

Hacker 2:

ETH Address: 0x8d08aAd4b2BAc2bB761aC4781CF62468C9ec47b4

BTC Address:
bc1qw5g8lw4kzltpdcraehy2dt6dqda8080xd6vhl4kg4wwsypwerg9s3x6pvk

- Hacker 2 was the other suspected entity involved in the breach. There were subsequent transactions observed moving funds to this address from Hacker 1's address.
- The nature of this breach could be described as well-planned and coordinated.
- The breach involved multiple unauthorised transactions from Deribit's wallets to external addresses.
- The rapid movement of funds, both in Ethereum and Bitcoin, combined with the splitting of assets across multiple addresses indicates that this was an attempt by the hackers to hide their tracks and slow down the tracing of the stolen assets.
- The significant amount involved in this breach underscores the severity of the incident and highlights the challenges faced by crypto exchanges in ensuring the highest level of security of their and their customer's assets.

Incident Details

Note: I used Etherscan and Blockchain.com/Explorer to look up and search for all these transactions.

Transaction Amounts:

Ethereum:

- 6,947 ETH transferred from Deribit to Hacker 2 on November 1, 2022, at 23:57:11 UTC.
- 20 ETH transferred from Deribit to Hacker 2 on November 2, 2022, at 01:14:47 UTC.
- 0.65 ETH transferred from Deribit to Hacker 2 on November 2, 2022, at 00:17:23 UTC.
- 9,080.1867 ETH was transferred from Hacker 2 to an unknown recipient on November 2, 2022, at 00:27:23 UTC.
- 31.4045 ETH transferred from Hacker 2 to an unknown recipient on November 2, 2022, at 08:35:23 UTC.

USDC:

- 14,727.9 USDC transferred from Deribit to Hacker 1 on November 2, 2022, at 01:47:47 UTC.

- 3,400 USDC transferred from Deribit to Hacker 1 on November 2, 2022, at 01:19:47 UTC.
- 14,727.9 USDC transferred from Hacker 1 to an unknown recipient on November 2, 2022, at 01:47:47 UTC.
- 3,400 USDC transferred from Hacker 1 to an unknown recipient on November 2, 2022, at 01:19:47 UTC.
- 14,727.9 USDC transferred from Hacker 2 to an unknown recipient on November 2, 2022, at 01:47:47 UTC.
- 3,400 USDC transferred from Hacker 2 to an unknown recipient on November 2, 2022, at 01:19:47 UTC.

Bitcoin:

- 691 BTC transferred from 105 Deribit addresses to Hacker 1 on November 2, 2022, at 10:56:11 UTC.
- 0.13 BTC was transferred from 26 Deribit addresses to Hacker 1 on November 2, 2022, at 11:08:16 UTC.

Parties Involved:

- **Deribit Exchange**: The victim of the unauthorised withdrawals.
- **Hacker 1**: Suspected entity behind the initial unauthorised withdrawals.
- **Hacker 2**: Suspected entity involved in receiving the stolen assets from Hacker 1.

Relevant Addresses:

Deribit Exchange:

Ethereum: 0x58F56615180A8eeA4c462235D9e215F72484B4A3

Hacker 1:

Ethereum: 0xb0606F433496BF66338b8AD6b6d51fC4D84A44CD

Bitcoin: bc1q2dequzmk5vk8nmmrata8nq4y0zgqn4vc0n2h8y

Hacker 2:

Ethereum: 0x8d08aAd4b2BAc2bB761aC4781CF62468C9ec47b4

Bitcoin: bc1qw5g8lw4kzltpdcraehy2dt6dqda8080xd6vhl4kg4wwsypwerg9s3x6pvk

Transaction Hashes:

Ethereum:

- 0xa1822e68a736bcdb57d05b2679260904813efdd17df62ede1d716dec9eeb4e8c: 6,947 ETH from Deribit to Hacker 2.
- 0xa43beda2d8739c679012b26b8b5f66dc4b7196eb31e39d6f7cdbede134e19720: 20 ETH from Deribit to Hacker 2.
- 0xe0d5d4798d4d4468c4a4df1c455b59c8dbe93195f75f988ae4e230743e15d2b6: 0.65 ETH from Deribit to Hacker 2.
- 0xdd608c8c4e8d8529967955d89f9e71842e80c3c84d592c72054f: 9,080.1867 ETH from Hacker 2 to an unknown recipient.
- 0xf3a14bfddc65725b4a345e0bafa84afd328de1b9487339157a0f24c9085b66f2: 31.4045 ETH from Hacker 2 to an unknown recipient.

USDC:

- 0x59f90e381121e516560972f6c07d1a95c82ba1dcc0c245c7efd6be7f767e3369: 14,727.9 USDC from Deribit to Hacker 1 and from Hacker 1 and Hacker 2 to unknown recipients.
- 0x223ae18897927db102cc0560277adeb3fe065f4523697bb67f6e8fe07feada39: 3,400 USDC from Deribit to Hacker 1 and from Hacker 1 and Hacker 2 to unknown recipients.

Bitcoin:

- Transaction ID: 6ff6-0e61: Transactions between Hacker 1 and Hacker 2.
- Transaction ID: 9793-d4cc: Transaction to Hacker 1.
- Transaction ID: b842-f7a2: Transaction to Hacker 1.

Tags:

Deribit Exchange: Tagged as "Exchange".

Hacker 1 and Hacker 2: Tagged as "Hacker Wallet".

Red Flags:

- Very quick movement of large amounts of cryptocurrencies in a short time
- Splitting of assets across multiple addresses to obfuscate the trail.
- The entirety of the stolen Ethereum was moved from Deribit to Hacker 2 within a short time, indicating an attempt to distance the funds from the initial breach.
- The Bitcoin transactions involved large sums being moved in quick succession, suggesting a coordinated effort to move the stolen assets swiftly.

Transaction Analysis and Visualisation

Analysis of Transactions and Associated Blockchains:

Ethereum Blockchain:

Transactions: The Ethereum blockchain recorded several large transactions from Deribit's wallet to the hackers' addresses. These transactions involved significant amounts of ETH and USDC.

Smart Contracts: The USDC transactions indicate the involvement of Ethereum's smart contract functionality, as USDC is an ERC-20 token.

Bitcoin Blockchain:

Transactions: The Bitcoin blockchain showed significant BTC transfers between the hackers' addresses. Unlike Ethereum, bitcoin transactions do not involve smart contracts.

Unusual patterns:

- Rapid Movement of Funds: Large amounts of cryptocurrencies were moved in a short time frame, indicating some sort of rush to move funds out of the compromised wallets.
- Asset Splitting: The hackers split the stolen assets across multiple addresses to make it hard to trace.
- Consistent Amounts: The repeated transfer of specific amounts such as 14,727.9 USDC suggests that this was an automated or coordinated action.

Details on Transactions

a) Source of funds

The primary source of the stolen funds is Deribit’s hot wallet. This wallet is used by the exchange to facilitate user withdrawals and deposits.

b) Purpose of transactions

Initial Unauthorised Withdrawals: The primary purpose of the initial transactions from Deribit's wallet to the hackers' addresses was an unauthorised withdrawal of assets.

Subsequent Transfers: The hackers then moved the stolen assets to other addresses, likely to distance the funds from the initial breach and to distribute them for potential cash-out or laundering activities.

c) Hidden information in Transaction Data:

Ethereum 'input' Text: The 'input' data in Ethereum transactions can contain information about the operations performed. For ERC-20 token transfers, like USDC, the 'input' data typically contains the method ID for the "transfer" function, followed by the destination address and the amount. Decoding this data can provide insights into the transaction's intent and the involved parties.

Bitcoin Transactions: Bitcoin transactions do not have 'input' data in the same way Ethereum does.

Visualise path information of illicit funds:

Ethereum Transactions:

Note: We were unable to use our previous assignments visualisation tool for the following reason:

1. FastAPI server issues: When trying to run the FastAPI server (via Anaconda) we ran into issues we were unable to resolve in due time, and for the sake of this assignment, we decided to use external visualisation techniques.
2. Neo4j Aura difficulties: We were having difficulties trying to create a query that would create all the required addresses as Nodes and create the relationships between them with accurate data.

   Due to this, we deemed that it was acceptable to use another tool for this assignment task. (diagrams.net)

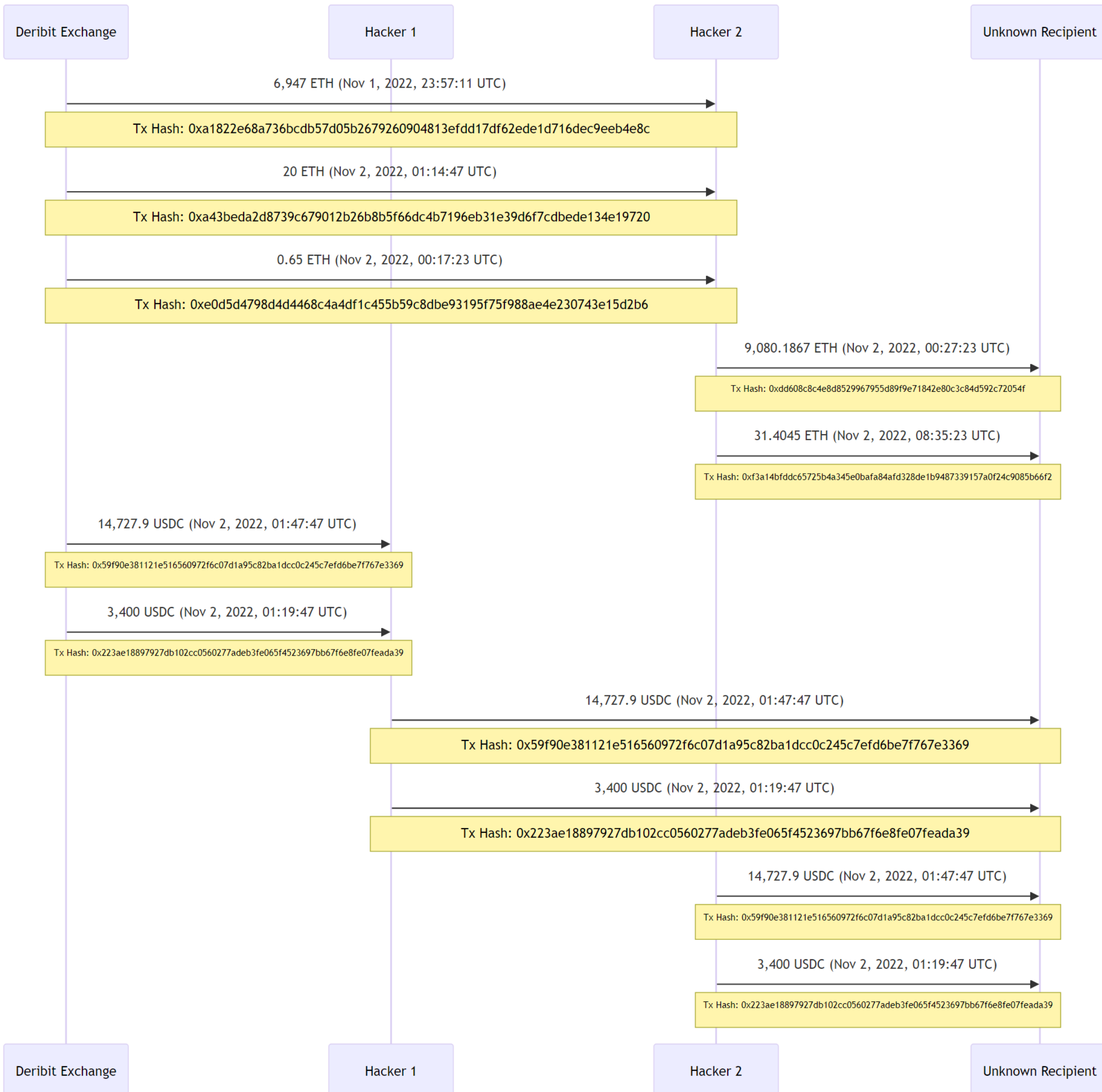


Diagram Explanation: The diagram visualises the flow of Ethereum and USDC between different entities.

Deribit Exchange: The victim of unauthorised withdrawals.

- Transferred 6,947 ETH, 20 ETH, and 0.65 ETH to Hacker 2.
- Transferred 14,727.9 USDC and 3,400 USDC to Hacker 1.

Hacker 1: Suspected entity behind the initial unauthorised withdrawals.

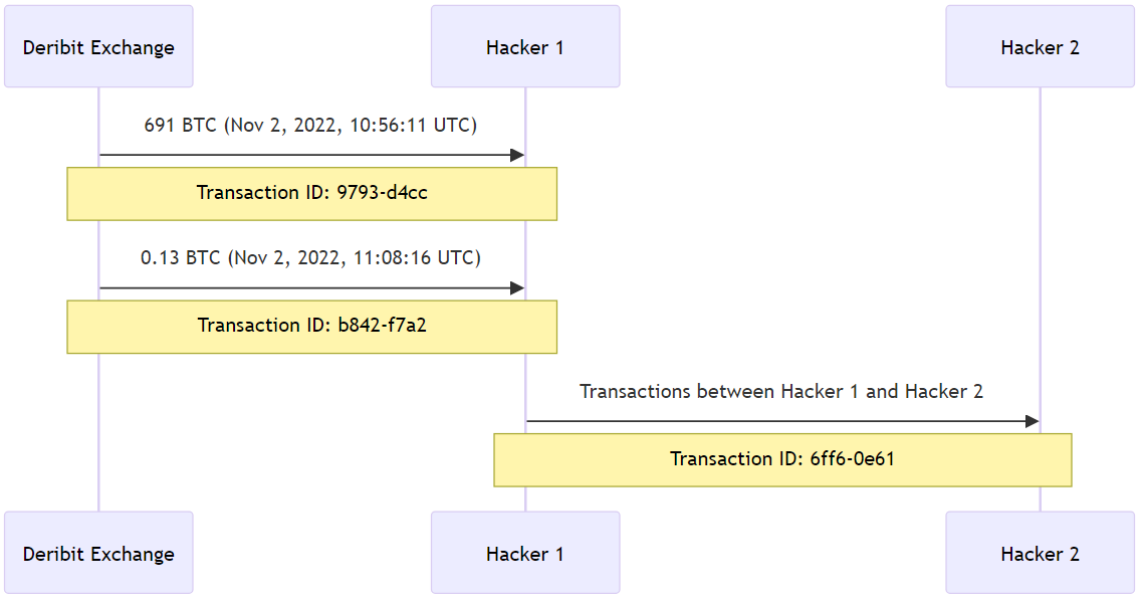
- Received 14,727.9 USDC and 3,400 USDC from Deribit Exchange.
- Transferred these amounts to an unknown recipient.

Hacker 2: Suspected entity involved in receiving the stolen assets.

- Received 6,947 ETH, 20 ETH, and 0.65 ETH from Deribit Exchange.
- Transferred 9,080.1867 ETH and 31.4045 ETH to an unknown recipient.
- Also transferred 14,727.9 USDC and 3,400 USDC to an unknown recipient.

Unknown Recipient: The entity that received the transferred assets from Hacker 1 and Hacker 2.

Bitcoin Transactions:



Mitigation Measures and Remediation

1. Actions taken to mitigate risks with suspicious/illegal activity.
    - Immediate isolation of affected wallets; Deribit moved quickly to remove the compromised hot wallets from the network.
    - User notification and password resets: All users received an emergency notification telling them of the breach, and they needed to reset their passwords and were strongly recommended to implement two-factor authentication.
    - Hiring a cybersecurity firm: A forensic investigation was conducted by a cybersecurity firm.
    - Withdrawals temporarily suspended: To protect users' assets, Deribit temporarily suspended the withdrawal service.
    - Law enforcement involvement: The breach was reported to both local and foreign law enforcement organisations, and a formal investigation has been launched.
2. Steps for ongoing monitoring and remediation.
    - Routine security audits: Both scheduled and unannounced security audits will be performed to look for any potential vulnerabilities inside their exchange or network.
    - Real-time monitoring: More advanced monitoring and alarm systems will be introduced to detect suspicious activity and immediately notify the security staff.
    - User education: To educate users on the best security practises, a series of FAQs, videos, and tutorials will be made available offered.

3. Recommendations for strengthening AML processes and controls.
    - Improving the KYC procedure: The current verification process should be improved to include more strict verification stages and background checks.
    - Advanced machine learning techniques should be utilised to examine transaction patterns and automatically flag any suspicious activity.
    - Ongoing AML Training: All employees must receive regular AML training to ensure that they are up to date on the current rules and risk factors.
    - Collaboration with regulatory agencies: Deribit must have a deeper involvement with regulatory bodies to guarantee that all AML procedures are followed. policies are compliant with current laws, and to protect future customers.

Bibliography

Godbole, O 2022, ‘Crypto Options Exchange Deribit Registered Record Trading Volume in November’, *Coindesk.com*, CoinDesk, viewed 16 October 2023, <https://www.coindesk.com/markets/2022/12/08/crypto-options-exchange-deribit-registers-record-ether-trading-volume-in-november/>.

Wan, S 2022, ‘Hackers attack Deribit hot wallets, steal $28M in crypto’, CryptoSlate, viewed 23 October 2023, <https://cryptoslate.com/hackers-attack-deribit-hot-wallets-stealing-28-milllion-in-crypto/>.

‘OKLink | The Best Multi-crypto Blockchain Explorer & Search Engine’ 2019, OKLink, viewed 23 October 2023, <https://www.oklink.com/>.

‘Blockchain.com | Be early to the future of finance’ 2023, Blockchain.com, viewed 23 October 2023, <https://www.blockchain.com/en/>.

etherscan.io 2023, ‘Ethereum (ETH) Blockchain Explorer’, Ethereum (ETH) Blockchain Explorer, viewed 23 October 2023, <https://etherscan.io/>.

free 2023, ‘Flowchart Maker & Online Diagram Software’, Diagrams.net, viewed 24 October 2023, <https://app.diagrams.net/>.