TÉCNICO LISBOA

Data Analytics for Blockchain Forensics

André Alexandre Pacheco Martinez

Thesis to obtain the Master of Science Degree in

Segurança de Informação e Direito no Ciberespaço

Supervisor: Prof. Miguel Nuno Dias Alves Pupo Correia

Examination Committee

Chairperson: Prof. Carlos Manuel Costa Lourenço Caleiro

Supervisor: Prof. Miguel Nuno Dias Alves Pupo Correia

Members of Committee: Prof. Nuno Miguel Carvalho dos Santos

October 2022

I declare that this document is an original work of my own authorship and that it fulfils all the requirements of the Code of Conduct and Good Practices of the *Universidade de Lisboa*.

Dedicated to my family and friends...

Acknowledgements

I would like to thank my thesis supervisor Miguel Nuno Dias Alves Pupo Correia for supporting me throughout the development of my thesis and to whom I dedicate the success of this project and also my family and friends who gave me the necessary support to finish this work.

Abstract

Blockchain has been given a major focus in recent years as its innovating technology has revolutionized the way information is stored on a decentralized way on its network and the speed at which as its transactions are executed that would normally take days on traditional banking.

A major problem is surfacing in this space, as cybercriminals use this technology for their own benefit stealing millions of crypto assets free of charge.

This work will focus on explaining how cybercriminals execute their schemes on the blockchain network, showing step by step the process on how they launder money on this network and providing a methodology on how to gather proof on the blockchain network and a tool to gather the overall information of the analytics of multiple projects and analyse their smart contracts to see if they are exploitable or safe for investors.

We will also focus on the mixer Tornado.Cash that I believe in the following years will be the main mixer used by cybercriminals due to his technology in keeping the cybercriminal hidden due to zk-Snark technology and its evolution that makes it really hard to follow them.

Keywords

Blockchain, Cybercrminals, Smart Contracts, Mixer, Zk-snark

Resumo

Nos últimos anos, a Blockchain tem sido alvo de grande atenção, uma vez que a sua tecnologia inovadora tem revolucionado a forma como a informação é armazenada de forma descentralizada na sua rede e a velocidade a que as suas transacções são executadas, o que normalmente levaria dias na banca tradicional. Um grande problema está a surgir neste espaço, uma vez que os cibercriminosos utilizam esta tecnologia para o seu próprio benefício, roubando milhões em criptoactivos e impunes dos seus crimes.

Este trabalho irá concentrar-se em explicar como os cibercriminosos executam os seus esquemas na blockchain, mostrando passo a passo o processo de como lavam dinheiro nesta rede e fornecendo uma metodologia sobre como recolher provas na blockchain e uma ferramenta para recolher a informação global de múltiplos projectos e analisar os seus contratos inteligentes para ver se são exploráveis ou seguros para os investidores. Vamos também concentrar-nos no misturador Tornado.Cash que acredito que nos próximos anos será o principal misturador utilizado pelos cibercriminosos devido à sua tecnologia em manter o cibercriminoso escondido devido à tecnologia zk-Snark e à sua evolução que torna realmente difícil segui-los.

Palavras-chave

Blockchain, Cibercriminosos, Contratos Inteligentes, Misturador, Zk-snark

List of Figures

List of Tables

List of Symbols

BC: Binance Chain

BEP: Binance Chain Evolution Proposal

BNB: Binance Coin

BSC: Binance Smart Chain

BTC: Bitcoin

CEX: Centralized Exchange

DeFI: Decentralized Finance

DEX: Decentralized Exchange

ETH: Ethereum

EVM: Ethereum Virtual Machine

ICO: Initial Coin Offering

KYC: Know Your Customer

LCX.: Liechtenstein Cryptoassets Exchange

LND: LendingBlock

PoSA: proof-of-stake consensus model

P2P: Peer-to-peer

UI: User Interface

URL: Uniform Resource Locator

WBTC: Wrapped Bitcoin

Zk-SNARK: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

Chapter 1

1 - Introduction

Blockchains are secure and tamper proof digital ledgers [1] implemented in a distributed environment and usually without a central figure of authority. They allow users to record transactions in a shared ledger and in the blockchain network no transaction can be changed once published. In the beginning of the creation of the blockchain concept around 2008 when BTC was created the blockchain concept was combined with other technologies and computing concepts to create the cryptocurrencies we have today which is cryptocurrencies protected through cryptographic mechanisms instead of a central bank or other figures of authority.

The first blockchain [2] that follows this definition was Bitcoin. Inside the Bitcoin blockchain the information represents electronic money and is attached to an address. Bitcoin users can transfer information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to verify the validity of the transactions inside of the blockchain. The Bitcoin blockchain is stored and collaboratively managed by a decentralized and distribute participants. This, along with cryptographic mechanisms, makes the blockchain resilient to attempts to alter the information inside the public ledger. Blockchain technology is the foundation of cryptocurrencies, users utilize public and private keys to sign and securely transact within the system while keeping pseudonymity [3].

The first blockchain design was created by Nakamoto and has evolved since then with new types of blockchains with smart contracts [4]. That allows you to create decentralized applications inside blockchains or provide liquidity for decentralize finance. With this, some malicious people use these tools for their own benefit since creating their own tokens so they can steal the users who invested on that asset or exploit a vulnerability in a smart contract on a blockchain to take out the liquidity of a certain exchange exploiting a smart contract function and with that start swapping the tokens that they stole from that contract and then they send the stolen tokens to a private mixer so we can't initially track them.

Developers try to help fix this issue by using convolutional networks [5] to distinguish between good addresses and suspect addresses that could be involved in money laundering to help track suspected money flow. The problem with many of these tools is that they aren't open source [6] or require payment to be able to use their services [7] making it harder to develop solutions faster to address these problems.

To help analyse these projects and do smart contract audits on them I developed a software named CoinFetch that uses the CoinGecko and the Go + Security API to gather data analytics from the overall project such as price, volume, social media presence through the CoinGecko API and smart contract audits from projects in the BSC and Ethereum blockchain that tells us if the smart contract is safe or exploitable through the Go + Security API.I also developed the first documented forensic analysis of a

cryptocurrency scam and a smart contract exploit in the BSC and Ethereum blockchain.

Section 2 starts by giving a brief explanation on the overall topics to understand this work and an explanation of the Binance ecosystem and Tornado.Cash protocol, in Section 3 we see what has been done before in this area related to smart contract exploits, extraction of raw data from a blockchain and process that information to use in multiple ways and exploring the weaknesses of a mixer protocol do try to trace the individuals who use these services. Followed by Section 4 where I explain my tool CoinFetch and its applications followed by a forensic analysis of a case in the BSC and Ethereum blockchain. Finally, Section 5 gathers the conclusions of this work.

Chapter 2

2 - Background

In this chapter we will talk about in general terms what technology is involved in decentralized finance to understand the forensic procedure of this work. We will start by talking of what are data analytics following by what is an exchange. Then we will explain what's decentralized finance involving the AMM (Automatic Market Maker) and its interaction with the smart contracts and we will conclude the general terms section explaining what are mixers and zk-snark technology. Following that we will talk about the Binance ecosystem where most of these token scams happen due to popularity of the protocol and lows gas fees. Finally, we will conclude this chapter with an explanation of the Tornado.Cash protocol that cybercriminals use to clean the assets without trail.

2.1 - General Terms

In this section we will explain the terminology needed to understand this work and the decentralized finance ecosystem.

Blockchain Data analytics: Blockchain data analytics [8] is the process of collecting data, to be able to analyse and visualize that data on a graphic model to be able to get important information about users and transactions and visually represent that data to help make better decisions based on the information that is provided.

Exchange: An exchange is a place where securities [9] and commodities are traded and have options or derivatives to be able to bet on a possible outcome of an asset. There are two types of exchanges. The first one is CEX where they ask for your KYC to be able to identify their user and the second is DEX that don't require KYC and are used on decentralized finance. The core function of an exchange is to ensure correct and efficient trading and display the price information of securities and commodities that are on that exchange.

Decentralized finance: (DeFi) is a technology based on cryptocurrencies and blockchain for transactions without a middleman [10]. DeFi is revolutionizing finance by replacing legacy finance with P2P relationships that can provide decentralized financial services for banking, loans and mortgages at a much cheaper and faster rate.

Automated Market Maker: Automated market makers (AMMs) [11] are the individuals or financial groups that give liquidity for the exchanges to be able to operate in the financial markets to obtain the volume data that happens on those exchanges so they can make better decisions when trading multiple assets. On decentralized finance the AMM are the smart contracts since they are who provides the liquidity to be able to execute a transaction.

Smart contracts: Smart contracts are stored on the blockchain and are programs that operate when certain conditions are met that activates those contracts. They automate the result of the transaction used by the contract so that the participants can know the outcome of that contract according to the function they used, smart contracts also automate workflow by triggering future actions when conditions are met.

Swapping: Swapping consists of the trade of one cryptocurrency with a different one on a DEX [12]. Token swaps were designed to reduce the operating costs and the time required to trade one cryptocurrency for other. A token swap has two definitions within the crypto space. The first connotes the trading a cryptocurrency with another with relying of a CEX. The second definition of token swap is when migration happens between blockchains, the developers must make easy for the investors swapping to the new token of that different exchange, this process is known to be token migration.

Mixer: A mixer is a service that combines different streams of cryptocurrency. This improves the anonymity of transactions making it harder to trace. The user transfers the money to the mixing service, which mixes it with that of other users who deposited also in the mixing service and transfer the mixed cryptocurrency to their chosen address making it no connection between the original transaction and this address.

Zk-SNARK: The acronym zk-SNARK stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,” [13] and refers to proving possession of concrete information without revealing that information and without interaction between the one who proves the information and the one who checks if the information is accurate. For example, a man has two balls of different colours and tries to prove to a colour-blind person that those balls are different by asking to swap the balls behind is back; eventually if those balls are different the man should be able to distinguish those balls with a higher than 50% accuracy and make the colour-blind man believe that indeed they are different proving with this how the Zero-Knowledge work.

Hot wallets: A hot wallet [14] is a cryptocurrency wallet that is always connected to the internet and cryptocurrency network. Hot wallets are used to send and receive cryptocurrency, and they allow you to view how many tokens you have available to use.

Blockchain Bridge: Blockchain bridges are mechanism that support cross chain transactions [15]. Bridges are used to allow the interaction between multiple native coins from their respective blockchain in a different one. For example, BTC cannot be on the Ethereum blockchain due that Ethereum is a blockchain with smart contracts and BTC isn’t, so to solve that problem we create a derivate of that native coin that mimics the price of that original coin. In this case of BTC, we create its derivate on the Ethereum blockchain named WBTC and now we have a way to connect both blockchains together.

2.2 - Binance smart chain Ecosystem

In this section we will analyse the ecosystem inside of the Binance Smart Chain (BSC) [16]. BSC is a

blockchain that runs parallel to Binance Chain (BC). BSC was created to start using smart contracts since BC didn't use them.

The BC blockchain serves the following purposes: to be able to do transactions to send and receive cryptocurrencies, token creation control and the circulating supply in the network through multiple functions such as: creating coins, deleting coins and stack or unstake coins.

Binance Smart Chain (BSC) started working in September 2020 and they created their smart contract inspired mainly by the Ethereum smart contract design. When they were designing BSC they focused on four different aspects that are: Keeping the BSC and BC blockchain separated in case of them went down it wouldn't affect the other, creation of a stake model to guarantee the participation in voting on the BSC proposals and block creation and validation of the BSC, They have compatibility with Ethereum since they copied the general design of Ethereum smart contracts, they asked Ethereum for help for the BSC in which the difference is the BSC consensus mechanism is PoSA in which the users of the BSC can use their BNB to become validators on the BSC network and they developed cross chain mechanism to be able to easily connect between the BSC and BC. To be able to do transactions on the BSC we need to use something as gas to pay for the cost of the transaction that is the currency of that ecosystem and that's when we will use BNB that is the coin that Binance uses to pay for the gas fees.

Figure 1: Binance Coin (BNB) logo

BNB was created in July 2017. It started as an Initial Coin Offering to gather money from multiple investors and to do that, they would incentivize offering discounts on the trading fees on the Binance exchange using BNB to motivate investors to invest on their cryptocurrency. BNB now serves three purposes that are the following: Pay gas fees in the BSC network, to stake the BNB on the BSC and get rewards from it and to perform cross-chain transactions.

2.3 -Tornado.Cash

In this section we will analyse the mixer Tornado Cash [17] that is decentralized privacy protocol that is built on Ethereum. Users can deposit and withdraw tokens in addresses that are different from the ones that made or took the deposit, with this they increase transaction privacy between their deposit and withdrawal addresses.

The protocol creates a secret hash before admitting the deposit and the hash. When the user wants to withdraw their crypto, they input the secret hash to prove they are the one who deposited the funds. Since the funds go through the liquidity pools of Tornado Cash we can't connect the transaction of the person who deposited and the one who withdrawal providing privacy.

Tornado Cash [1]is owned in by its community since the ownership was transferred in 2020 when the developers gave their control to them making the protocol decentralized completely. Tornado Cash uses zk-SNARKs and is able to hide the transaction information making it untraceable and ready to be deposited on crypto wallets like Metamask or Trust Wallet. Using Zero proof the protocol improves its privacy by making the communication of transactions secure without revealing important transaction information.

Tornado Cash has anonymity mining designed to provide Tornado Cash with liquidity to be able to hide their transactions. The user by interacting with the Tornado Cash protocol receives points that are deposited on a protected account that can be used to convert them to TORN that's the currency used on the Tornado Cash protocol.

Tornado Cash was a popular protocol in the crypto space it came with a lot of controversy, the primary one occurred recently August 2022 when U.S. Treasury implemented sanctions for using this protocol. But these sanctions only started forming in March 2022 where Roman Semenov stated to Bloomberg News [18] that sanctions on decentralized protocols are impossible since there isn't a way to control a fully decentralized space.

The Treasury Department on August of 2022 applied sanctions taking down the Tornado Cash website and forbidding US users of using that protocol since the majority of transactions in there are supposed to be for money laundering purposes.

The Treasury Department stated that Tornado Cash was used for the money laundering that should be worth around of $7 billion in cryptocurrencies since the beginning of the protocol which it even includes a cryptocurrency theft by Lazarus group that goes around of 455$ million in multiple cryptocurrencies stolen. All currency that is taken out of Tornado Cash is now associated with the imposed sanctions of the Treasury Department and that implies that the exchanges or businesses that use Tornado Cash services will be considered to have the addresses who use those services tainted and the Treasury of

[1] https://github.com/tornadocash/tornado-core

Department should go after those individuals.

At the time of writing the Tornado Cash Website was taken down by the U.S Treasury but you can still use its services since it's on the Ethereum Blockchain if you have some understanding of how it works you can still use the mixing service. But lets us see how the website was to help us understand better the technology of it using the Wayback Machine [2] that is a service that allows to see snapshots of webpages that are no longer available.

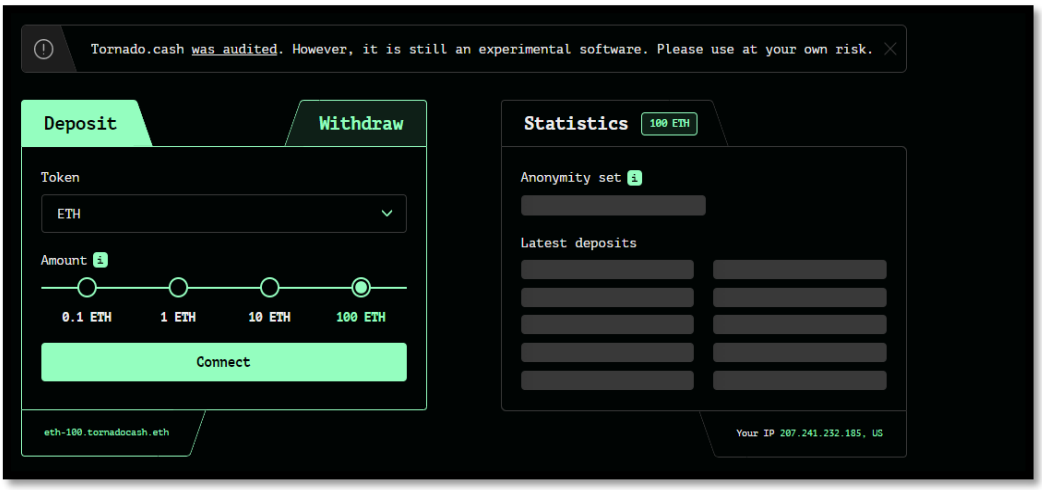


Figure 2: Tornado Cash Mixing Service

The person who wanted to use the mixing services, in the case of this work, cybercriminals after stealing set amount of tokens of different protocols of the liquidity pool and swapped them for Ethereum he would then send the Ethereum after connecting his wallet to this website depositing the Ethereum according to set quantity defined by the amount above and it would send the Ethereum to a Mixing pool and the cybercriminal would get a hash to recover the stolen Ethereum on an account defined by him and couldn't be traced since the tornado cash application is used as a 3rd party that sends the money to a new account not giving us a direct link of the stolen money. We can try to guess if an abnormal amount of Ethereum gets out of Tornado Cash soon after the theft that is stolen money with high probability but only a rookie cybercriminal would do that since in general, they would leave the money in the mixing process for some while to not be traceable. The solution that I was going to propose is what the U.S Treasury did that's making all accounts that interacted with this service suspicious and couldn't take out the money in an exchange that is linked to his KYC and would be easily caught since he wouldn't be able to explain with a sound explanation where did this money came from.

The other way to continue since the original site went down, is to use this service directly in the Ethereum Blockchain or the BSC Chain. We can do this through the smart contract that allows us to use the functions of Tornado Cash.

[2] https://archive.org/web/

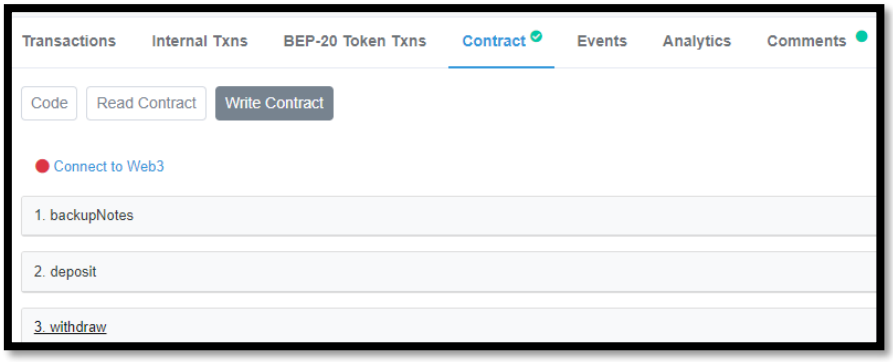


Figure 3: BSC Tornado Cash Proxy

Since the Tornado Cash site went down cybercriminals now use the blockchain directly connecting their wallet to the blockchain and then use the smart contract that was created to continue to use the services provided from Tornado Cash allowing them to deposit or withdraw the tokens they want. For a better look at this contract go to the Binance smart chain explorer (bscscan.com) and search this address 0x0D5550d52428E7e3175bfc9550207e4ad3859b17.

2.4 - Summary

In this section we presented the overall foundation to understand this work. In Section 2.1 we presented the general terms to understand decentralized finance and how to operate with it. In Section 2.2 we talked about the Binance ecosystem explaining its origins and how to works. Finally, in Section 2.3 we explored the origins of Tornado.Cash and how the mixer protocol work.

Chapter 3

3 - Related work

In this chapter we will see the work that has been done before in this area focusing on smart contracts exploits on the Ethereum Network showing us the different vulnerability's that a contract has. Followed by the analysis of a Ethereum raw data extracting tool to gather data analytics and the possible use cases that they give. Followed by a Monero analysis in trying to trace the user identity of the person who used the mixer and explain how they were able to find the vulnerabilities of that mixer that allowed for the traceability of those individuals. Finally, we will have a discussion about what has been done and what I will do to try to solve this problem.

3.1 - Smart Contract Exploits

In this section we will see types of exploits on a Ethereum smart contracts to have an understanding of what types of exploits a smart contract can suffer exposing their vulnerabilities. Smart contracts define what is allowed to do with them and who can interact with them, the most important case is when the contract will deposit on a user since in the case it has a vulnerability it can be exploited taking all the money also known as reentrancy attack [19].

When these types of contracts are vulnerable the attacker will steal portions or all the funds that were inside the contract which will result on a loss of assets for the owner of the contract. To identify such vulnerabilities in these contracts we need to analyse the contracts code to reveal critical vulnerabilities that might be used to withdraw the funds of those contracts. The hackers are able to do this due to four critical EVM instructions and we can label these four instructions into two categories: The first two instructions cause a direct transfer of the contract and the other two instructions allow random execution of Ethereum bytecode within the context of those contracts.

3.1.1 – Direct Transfer

In this section we will explain two of the EVM instructions in the Ethereum smart contracts that allows the hacker to transfer an asset to a given address: Those instructions are CALL and SELFDESTRUCT. The CALL instruction performs a transaction. But if an attacker can control the direction in which that data its sent, they can cause the contract to transfer the asset to an address under the control of the hacker. The SELFDESTRUCT instruction is used to destroy a contract. This will cause the contract to stop working making it impossible to do more calls to. The SELFDESTRUCT instruction has an argument that allows to send all the funds to one address to one wallet after the destruction of the contract if there is a vulnerability that allows the hacker to use this function, he can steal those funds.

3.1.2 – Code Injection

In this section we will explain the other two EVM instructions CALLCODE and DELEGATECALL instructions which allow to execute code from 3rd parties contract. CALLCODE its similar to CALL, with the difference that it doesn't do a transaction to a different address, but rather to himself as if it had the code of another address but the contract who benefits of the new transaction it's still the same but it will be executed using the new address code. DELEGATECALL does the same process but it keeps the original information of the sender and the value. If a hacker controls the address of either CALLCODE or DELEGATECALL they can inject code into the contract and by deploying these instructions the hacker is able to destroy the contract and send the funds to his address.

3.2 - Extracting and Exploring Blockchain Data from Ethereum

In this section, we will see a blockchain data analytics framework named eXplore Blockchain ETH (XBlock-ETH) [20], that analyses Ethereum data. The tool gathers three types of Ethereum data that are blocks, traces, and receipts. This data will help researchers to investigate and analyse Ethereum data in a useful way.

3.2.1 - Data Extraction from Ethereum

In this section we will talk about the procedure of how the data was obtained from the Ethereum blockchain. When using this tool, it collects three types of blockchain data that as previously mentioned was block, receipt and trace. We can describe each of these fields as the following:

- **Block**: Block data is being kept in the Ethereum blockchain, each one of these blocks consists of two components the first one is the block header where it gathers the basic information of the block and the second component is block transactions where the body of the block is built.

- **Trace**: Trace data is the run-time data that was generated in Ethereum Virtual Machine. Trace data is referred to the data that is obtained during the execution and can be displayed in three types: Create obtains information about the creator of the contract, its code, and the balance that a smart contract starts when it is deployed. Call happens when cryptocurrencies or information are being transferred into different addresses in the Ethereum network, Reward happens when the miners on Ethereum mine a block and that reward depends of their contribution to mine it.

- **Receipt**: When the transaction is executed, some states on Ethereum have been changed and we need to know what was that changed that happened. To reduce the expenses of the users that use those smart contracts those contracts leave an Event that details what happened in that transaction and that can be read by the users.

3.2.2 - Data Applications of Ethereum

In this section we will explore the applications of the data obtained from Section 3.2.1 and see the possible uses of XBlock-ETH that focus on these three areas: Blockchain System Analysis, Smart Contract Analysis and Cryptocurrency Analysis.

- **Blockchain System Analysis:** The XBlock-ETH can process data from blockchains and can use it to focus on these types of blockchain system analysis that are: decentralized analysis since its data offers a good overall understanding of the transactions that happened on Ethereum making us obtain multiple data for decentralized analysis and predicting gas price costs making the users save a lot of cost fees paying the minimum required to do that transaction and not pay extra gas for the transaction.

- **Smart Contract Analysis**: The XBlock-ETH can be used in the studies of smart contracts in these different areas that are: Similarity between contracts since there is a great similarity between the smart contract codes and the calling of those codes making the developers able to know what would be the user experience before hand, detection of vulnerability in contracts since a number of malicious attacks on the Ethereum blockchain have made investors lose huge losses in cryptocurrency assets, detection of fraud since smart contracts are used by a lot of investors they can be used to scam them and example of these would be ICO contracts with vulnerabilities to exploit the contract and go away with their money and being able to detect that fraud would safeguard a lot of investors.

- **Cryptocurrency Analysis:** XBlock-ETH can be used to analyse cryptocurrency in the following three fields: Crypto transaction analysis of cryptocurrency transactions to capture the order flow of those transactions to help us detect possible money laundering schemes, Analysis of cryptocurrency prices in which price analysis consists of three steps that begin by collecting the price information from exchanges, find patterns between the price to be able to help make better decision making and predict possible future prices to obtain profit. The last field is fake user detection that its used to detected possible fake users that are used to improve the activity ranking of a project to make investors believe the project has more activity that it actually has.

3.3 - Empirical Analysis of Traceability in Monero

In this section we will see the work done in trying to trace the transaction flow in the Monero mixer [21]. Monero is a privacy-oriented cryptocurrency that is focused in hiding the identity of its users by including worthless coins called mixins to camouflage the actual coins that are spent. The author evaluated two weaknesses in the Monero's mixin strategy. The first weakness is that about 62% of the transaction inputs with mixins are vulnerable to be found by process of deduction and with this, actually find the real input that was used to send the real coins and the second weakness is that Monero mixins are able to be distinguish by the age of when those coins were created and with this identify with a high degree of

confidence the real input of that transaction.

3.3.1 – Monero Weaknesses

In this section we will explain in more detail what each of these two weaknesses are in the Monero Blockchain.

- **Weakness 1:** The first weakness focusses on that most prior transactions before February of 2017 don't contain any mixins at all since by default it was using zero mixings making them deducible and with this they don't have the privacy that they expect from this protocol and the majority of their transactions can be deducted and also provide a danger since the Monero protocol doesn't take account if the mixings were previously used before we can associate their transaction with a previous output.
- **Weakness 2:** The second weakness focusses on that the mixins that are given for the user to use arent random but instead come from a rather specific pool making it easier to be identifiable since the most recent input is usually the real input of the transaction making it easy to be traced.

3.4 – Discussion

In this section after analysing the multiple Sections of Chapter 3 we learned how exploiting smart contracts worked, followed by learning to extract data from the Ethereum blockchain for data analytics purposes and how to possibly trace a mixer by exploring weaknesses in their protocol that allow us to trace their users. After analysing these works, we can see that their proposed solution doesn't provide a tool that allows us to gather the overall information of a cryptocurrency project and allows us to see if the smart contract its exploitable. It also doesn't provide a framework on how to directly read the blockchain transaction data to be able to follow these scams and with that my proposed solution is to be able to provide an open-source smart contract audit tool that also manages to gather the information of the project that we are searching to be easier to gather evidence and a framework on how to read BSC and Ethereum transaction flow data on the blockchain.

Chapter 4

4 - Blockchain analytics forensic analysis

In this section we will talk about the tool that I developed to help analyse blockchain data to make it easier to gather information about these projects and do audits to understand their exploits, CoinFetch, allows to gather information about multiple projects in the CoinGecko API and analyse if their smart contracts have vulnerabilities that can be exploited through the Go + Security API. Then we will see how cybercriminals exploits those smart contracts inside the blockchain to gain the privileges of a wallet and steal the money inside of it by calling functions to do it and how they work to exploit the contract. After that we will talk about the general overview of how they start the process of money laundering by swapping their tokens on a decentralized exchange to a unique coin, for example Ethereum, so they can send to a mixer to hide the money since we will only be able to see the relay, they launder the money and we can't track the account it went in making it extremely hard to locate where the money went. Finally, we will do a methodology and an evaluation of the results of this work.

4.1 – CoinFetch

In this section we will talk about the tool that I developed to search cryptocurrency scams information and help cryptocurrency users to audit smart contracts to see if they are safe for investment or if they have vulnerabilities that can be exploited by cybercriminals to steal cryptocurrency assets. CoinFetch is a tool that gathers information from two applications. The first one is CoinGecko that we use to gather information about crypto in general, this allows us to gather: price data, volume data, social media websites, contract address, Liquidity scores, the all-time high price and all-time low. The second application is Go + Security that we use to do the smart contract audits giving us different metrics to access the smart contract security such as: function to take back ownership of that contract, if it can change the balance of one of the tokens holders, if its a honeypot contract were this contract calls another function from a different contract, whether he can blacklist or whitelist a user, has the self-destruct function and have external calls to other contracts.

4.1.1 – User Interface

In this section we will talk about the overall functions on my tool that you can access on the user interface as you can see on Figure 4.

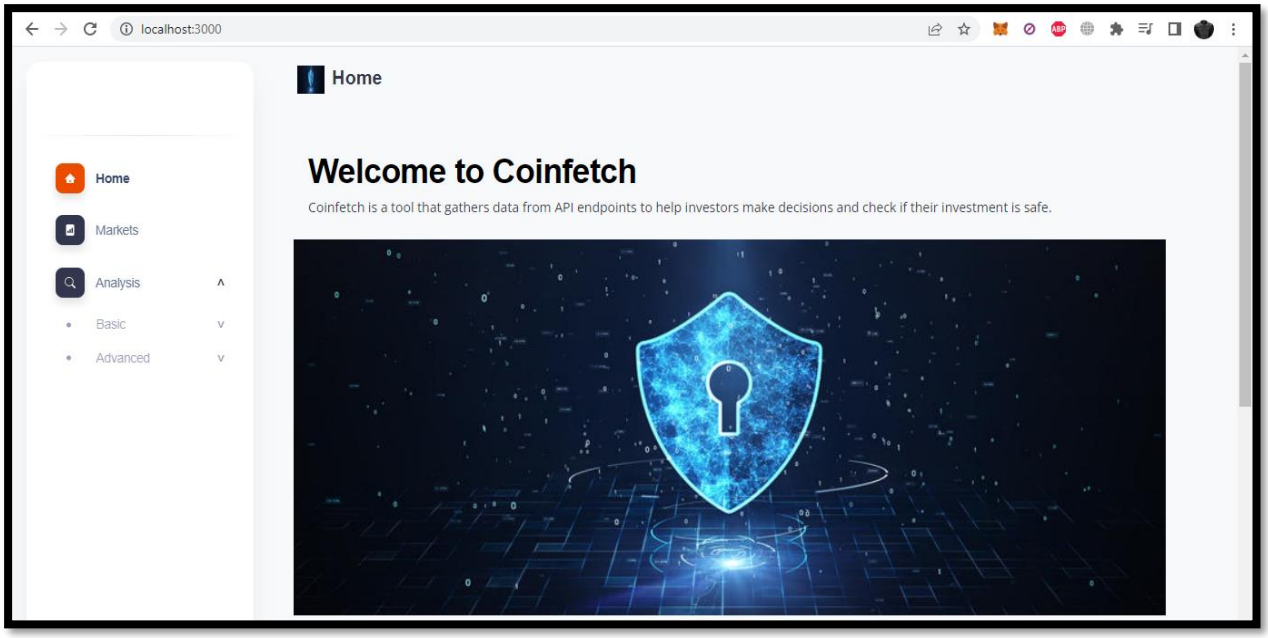


Figure 4: User Interface

This is the user interface consisting of the welcome page and on the left corner we see three functionalities the first one, Home, that makes you go back to the user interface at the beginning. The second function, Markets, allows us to see the top cryptocurrencies coins by market cap and allows us to see their change in price since the all-time high as you can see in Figure 5 to 6.

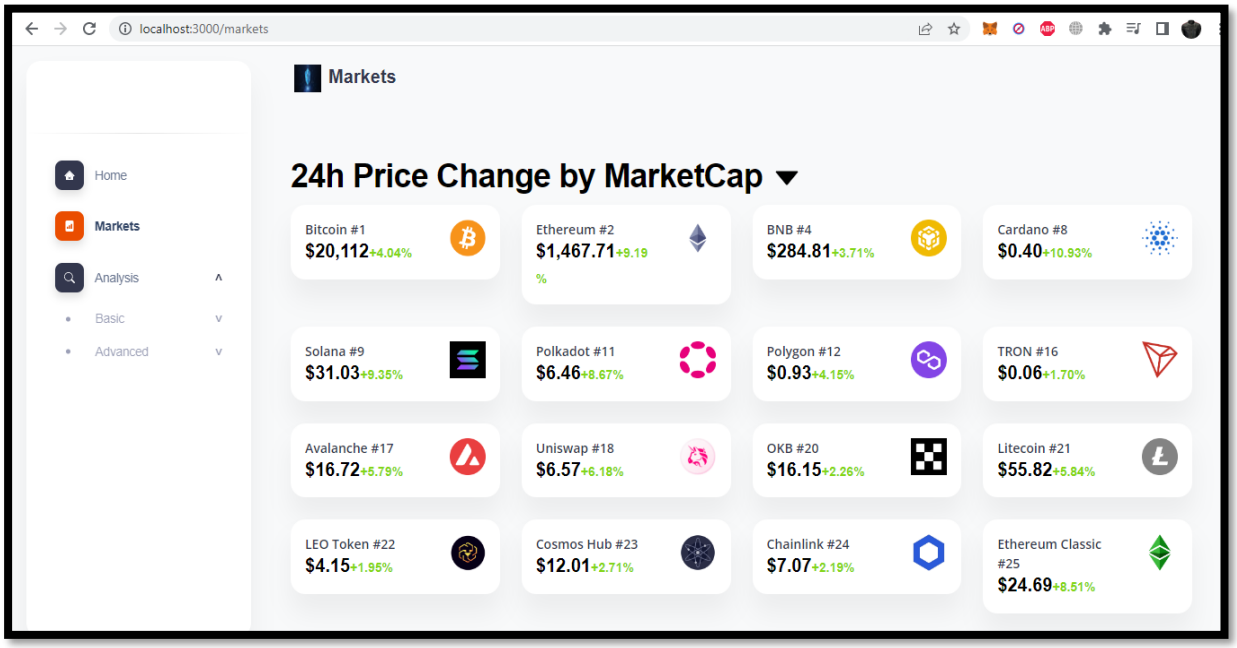


Figure 5: 24 h Price Change by MarketCap

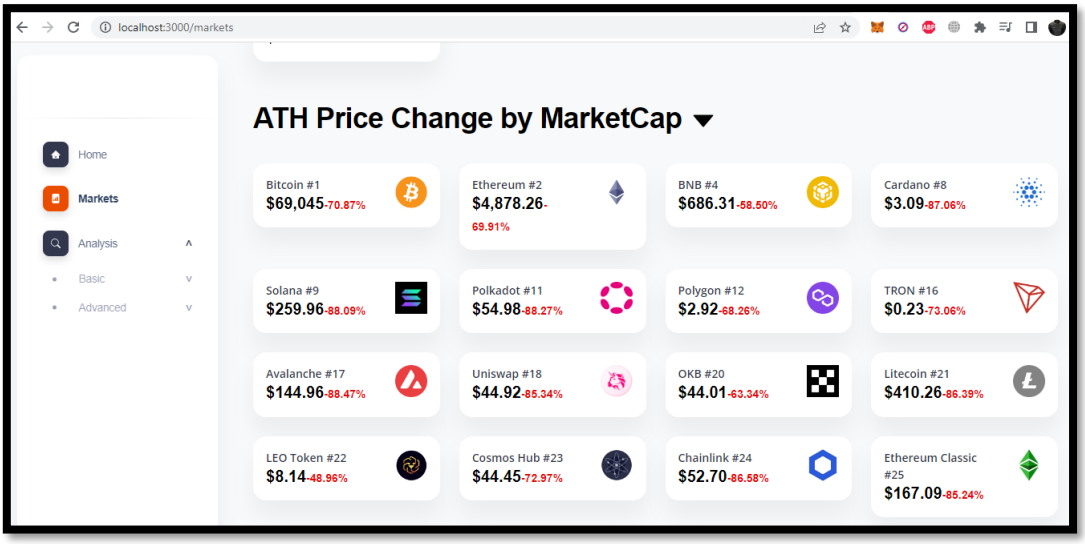


Figure 6: All time high price change by MarketCap

The last function is the Analysis function that consists in two parts. The Basic analysis searches the overall information of the project that we want in the BNB or ETH chain in the CoinGecko API. And the Advanced analysis that through the contract address given by CoinGecko API we can use the Go + security to gather that contract information and make a smart contract audit in that contract to see if it has vulnerabilities or not.

4.1.2 - Basic Analysis

In this section we will talk about Basic analysis functionality on my tool that consists in calling the CoinGecko API and gathers all the information about price, volume and social media websites, contract address, Liquidity scores, the all-time high price and all-time low. On Figure 7 you can see the Squid Game token scam that we will analyse on Section 4.2.

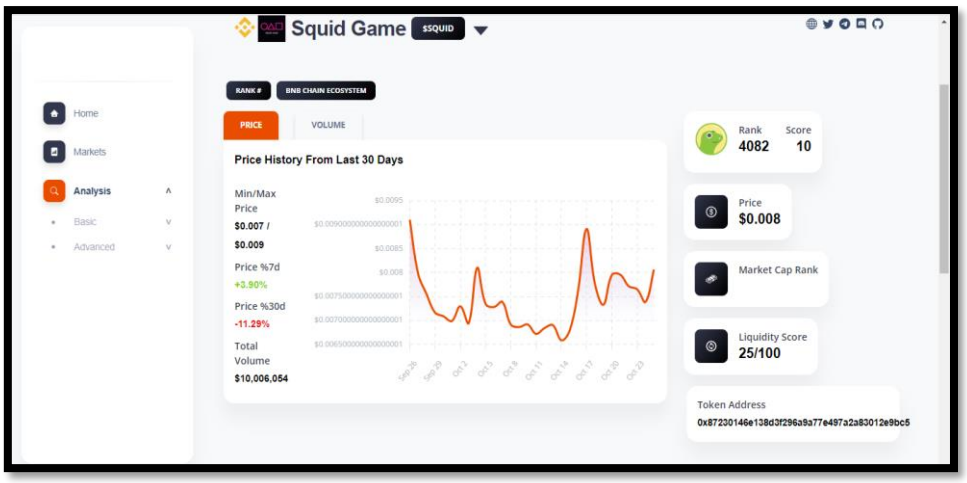


Figure 7: Basic analysis to gather information about Squid Game Token

4.1.3 - Advanced Analysis

In this section we will see the last functionality of my tool that consists in doing smart contract audits to smart contracts addresses that we gather through the CoinGecko API and using the Go + Security API from the information that we gathered we can do smart contracts audits that are compatible with the BSC and ETH blockchain. This function has two parts the Overall shows all the information, Contract audits, contract ABI and contract address we are analysing. The second is Security Information that only shows the information of the smart contract audit.

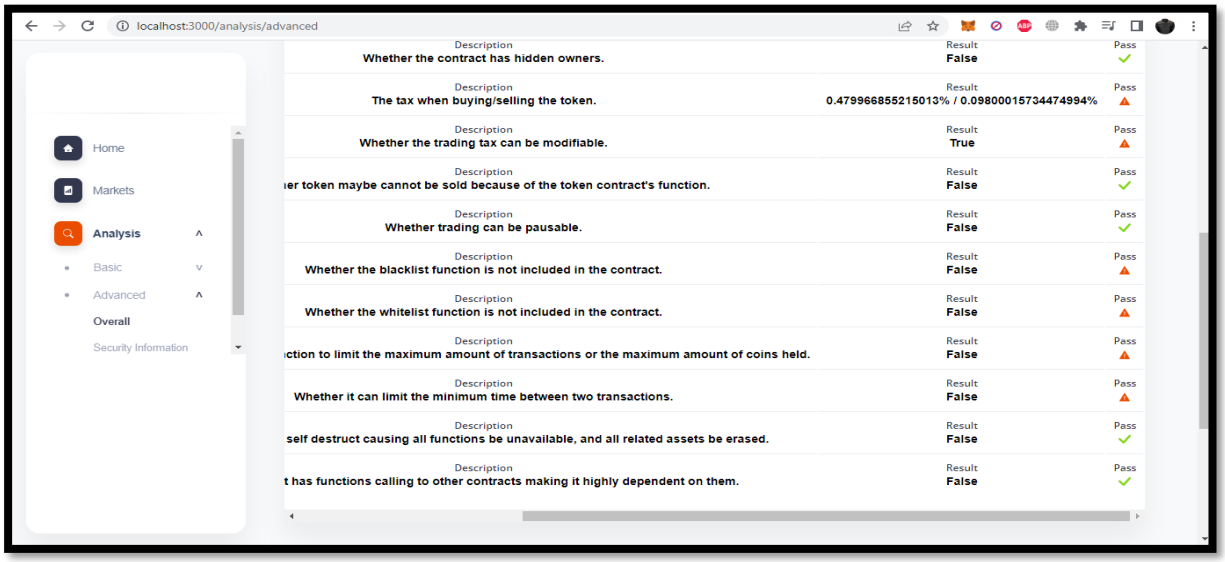


Figure 8: Smart Contract Audit using Go + Security

In Figure 8 you can see smart contract audit checking conditions with a true or false method to see if the cryptocurrency is safe to invest or the contract can be exploited, we also got on Figure 9 the smart contract ABI that links us to the code if available to read on the BSC or Ethereum chain.

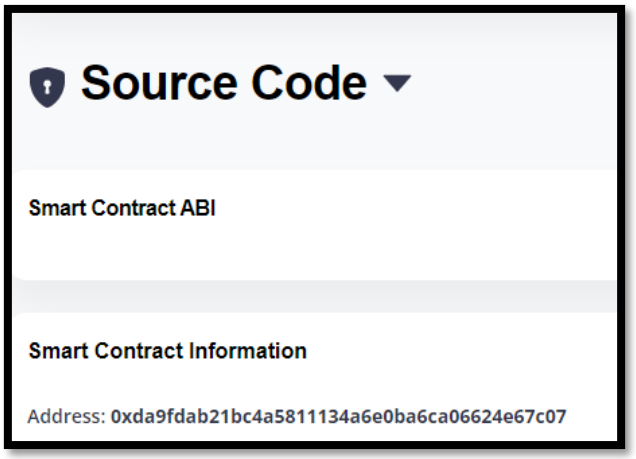


Figure 9: Smart Contract ABI to see contract source code and its address

4.2 Squid Game Token Scheme

In this section we will analyse the Squid Game Token scam that occurred between October and November of 2021 and was the first case that got major attention going to main stream media since investors weren't allowed to sell their tokens and that allowed the price of the token to soar from one cent to 3400 $ and collapsed to 0$ making investors loose around 3.38 million $ [22] but according to my investigations at the time of theft was actually 14 $ million if you sum the value of the stolen amounts in Section 4.2.2 . Using the CoinFetch tool we manage to gather the overall information of this project using the Basic Analysis from the tool Section 4.1.2 and then got the URL to their website and used the Wayback Machine to see how it used to look like. First, we will see how the Squid Game site was attractive for investors and how they would buy their tokens and then an in depth look on how the cybercriminal was able to do this.

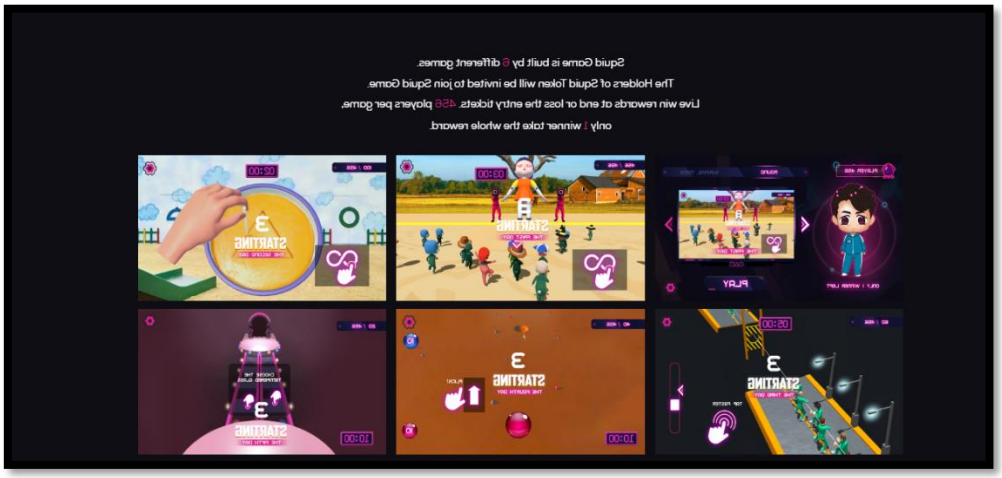


Figure 10: Squid game token website

The Squid game token initially would consist in 6 different games up to 456 players in which you needed to buy SQUID to be able to participate on the games. In the end only 1 player would remain and would win the others players tokens and make a profit from it. These games never happened; they even created another token called Marbles that stakes other tokens to gain Marbles that could be traded for more Squid Game tokens to play more games managing this way to steal even more money. They fooled investors with fake partnerships and people that don't even exist doing duties as CEO and other positions in this project.

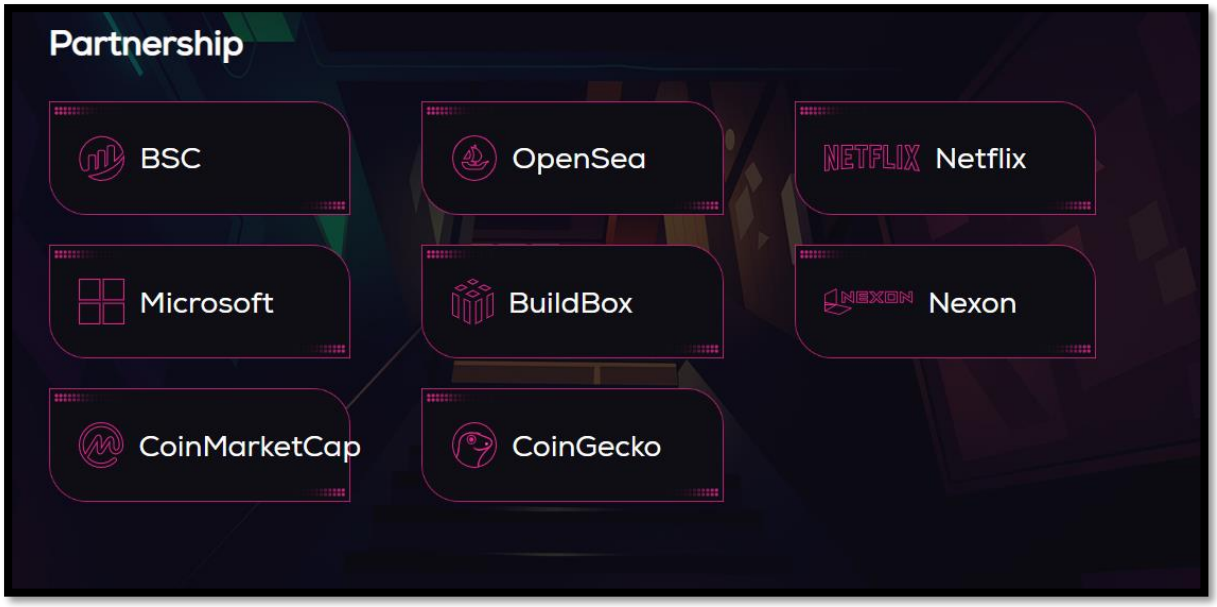


Figure 11: Fake partnerships

Investors seeing that this project was partner with Netflix and Microsoft didn't doubt that it was fake it only gave them more confidence that this project was in solid hands but unfortunately these companies never backup this project and these scams usually do this because the normal investor won't go looking to see if these statements are true.

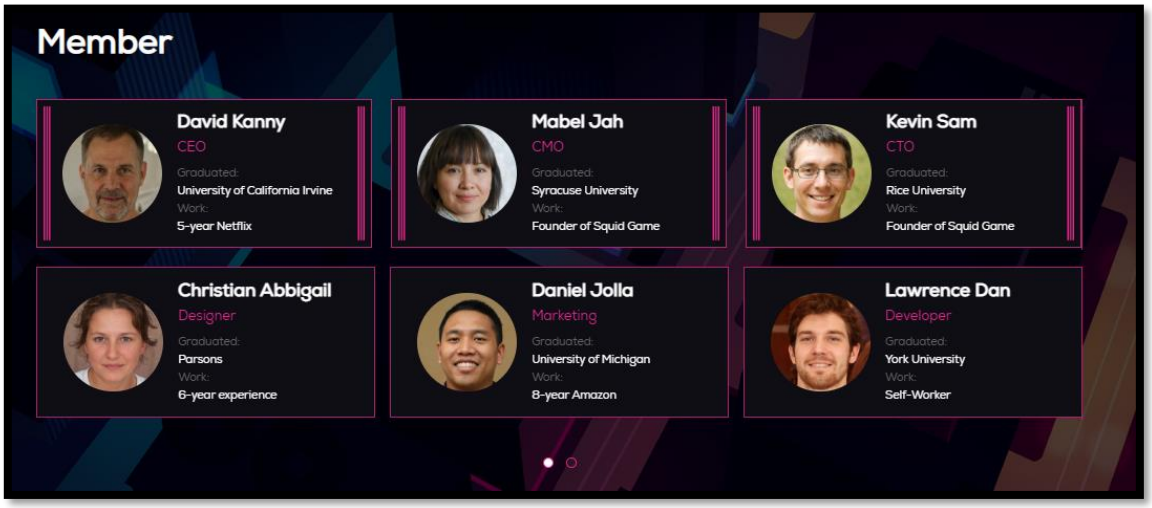


Figure 12: Fake people behind the project

A quick reverse image search we can see that these people don't exist. Cybercriminals used a service that was created by Nvidia to generate through an AI a person who isn't real fooling investors of the project to believe that these people actually existed[3].

[3] https://thispersondoesnotexist.com/

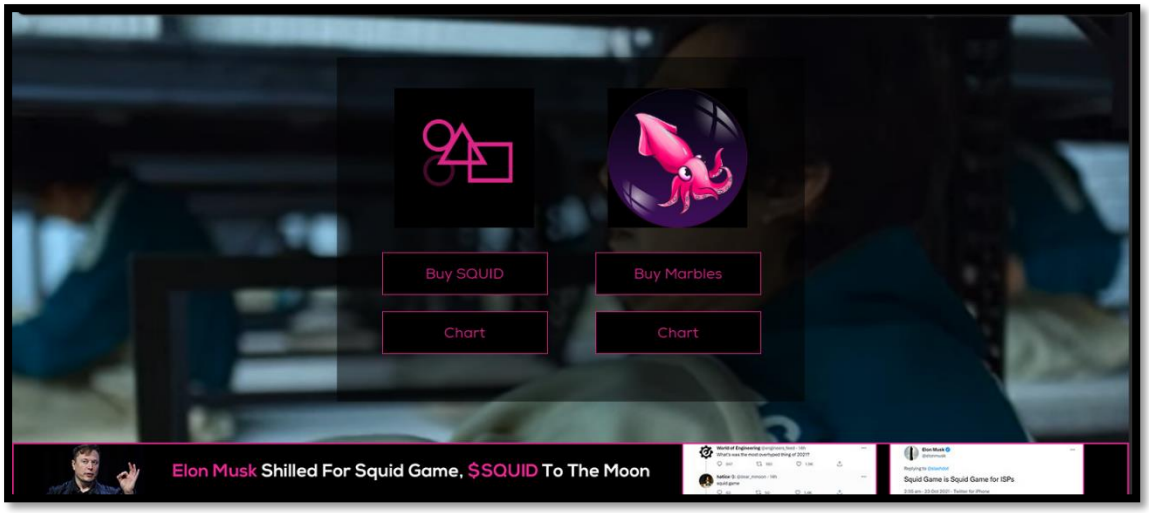


Figure 13: How to buy the Squid tokens

Investors after having read how to project worked then proceed to buy those tokens to earn the benefits of having them. When they clicked the buy button then they would be redirected to PancakeSwap to swap their BNB or other tokens for SQUID or the Marbles token.

PancakeSwap [23] is a decentralized exchange native to BNB Chain. In other words, it shares some similarities with established platforms like Uniswap in which the users can swap their coins for other coins without the input of middleman services. The only difference is that PancakeSwap focuses on BEP20 tokens that are a specific token standard developed by Binance.

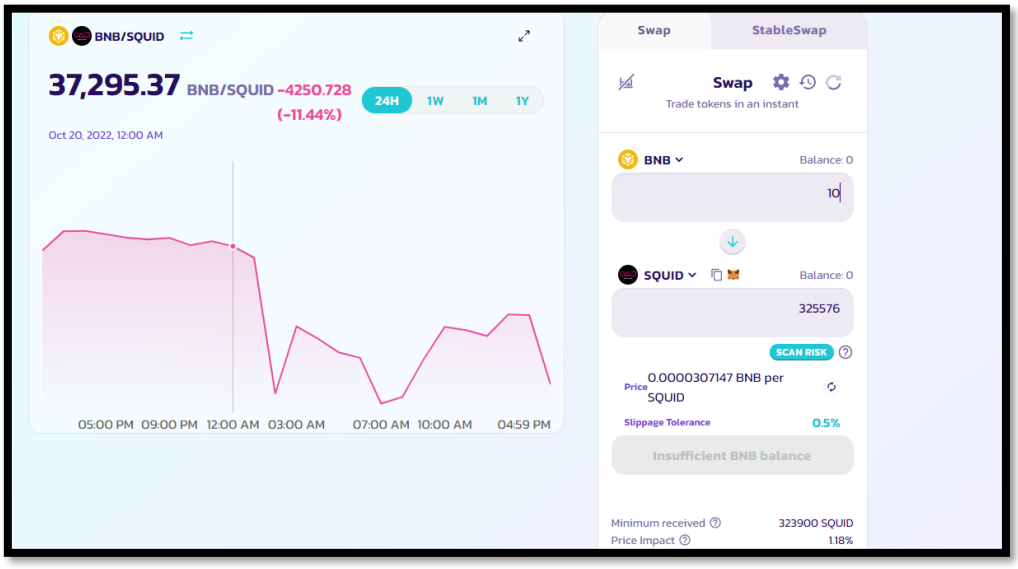


Figure 14: Swapping BNB for SQUID

After clicking on the buy button on the squid game token we were brought to PancakeSwap to Swap BNB for the SQUID or Marbles token (Squid in this case) and then we would have the Squid tokens only problem now is when investors tried to sell it, they couldn't and the cybercriminals run away with their money leading as this for a result.

Figure 15: All the liquidity stolen by the cybercriminals

These scams are usually tracked by the poopcoin[4] website that allows us to see pretty easily the general information that we will looking for on how this scam was started till the end in this case.

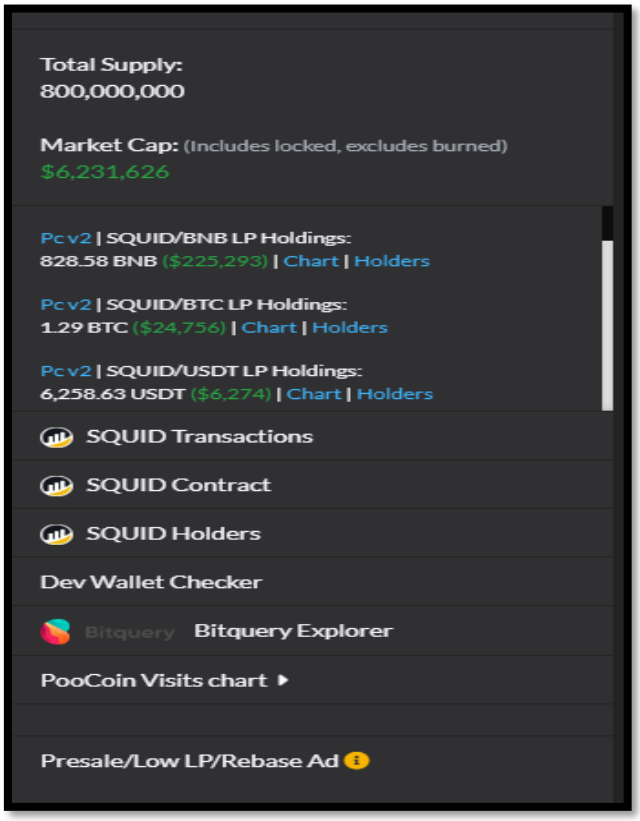


Figure 16: Key information to gather proof

In Figure 16 we obtain the essential links on how this scam was elaborate especially the SQUID Contract that allows to see how this contract worked and his interactions and the Dev wallet that was

[4] https://poocoin.app/

the creator of this scam.

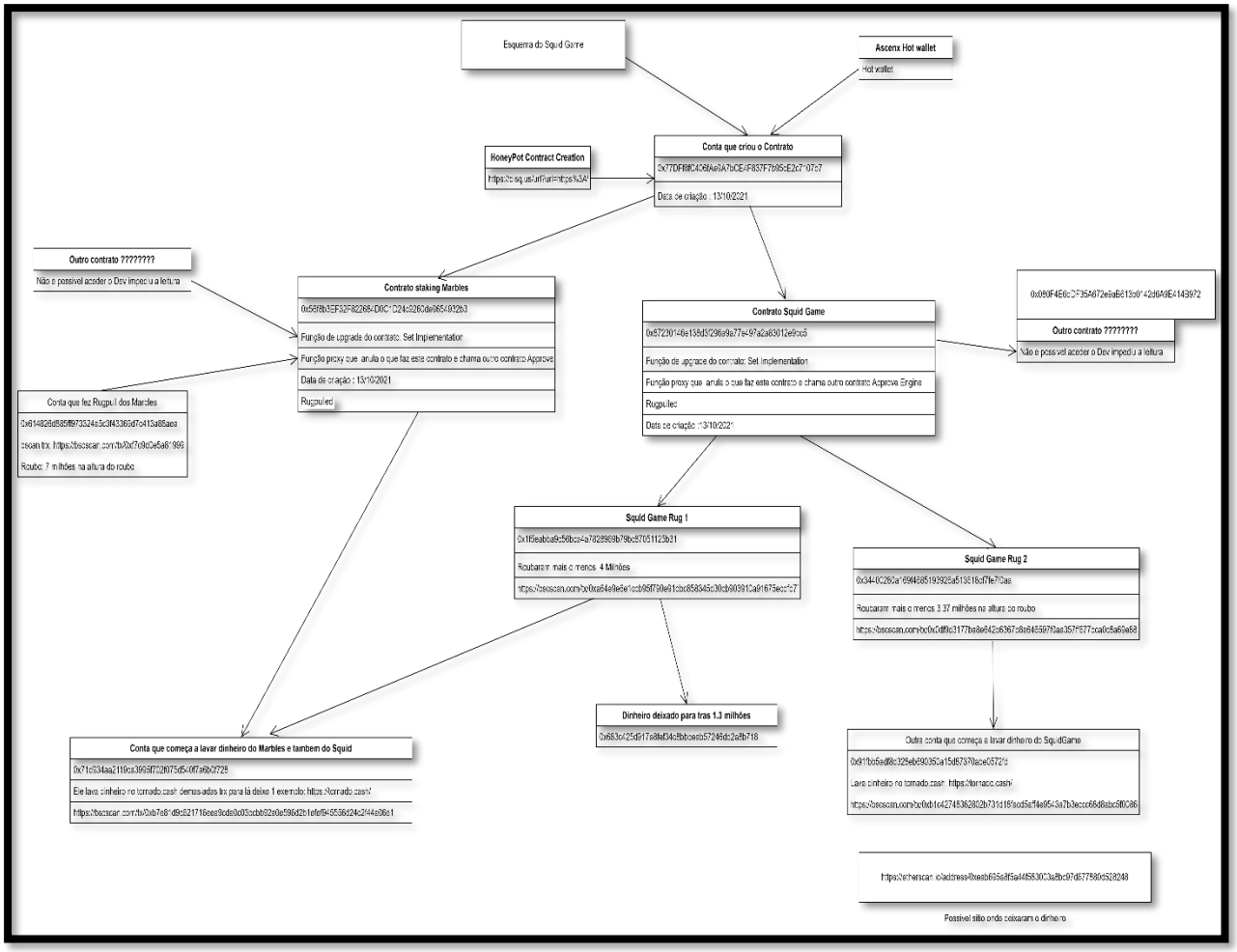
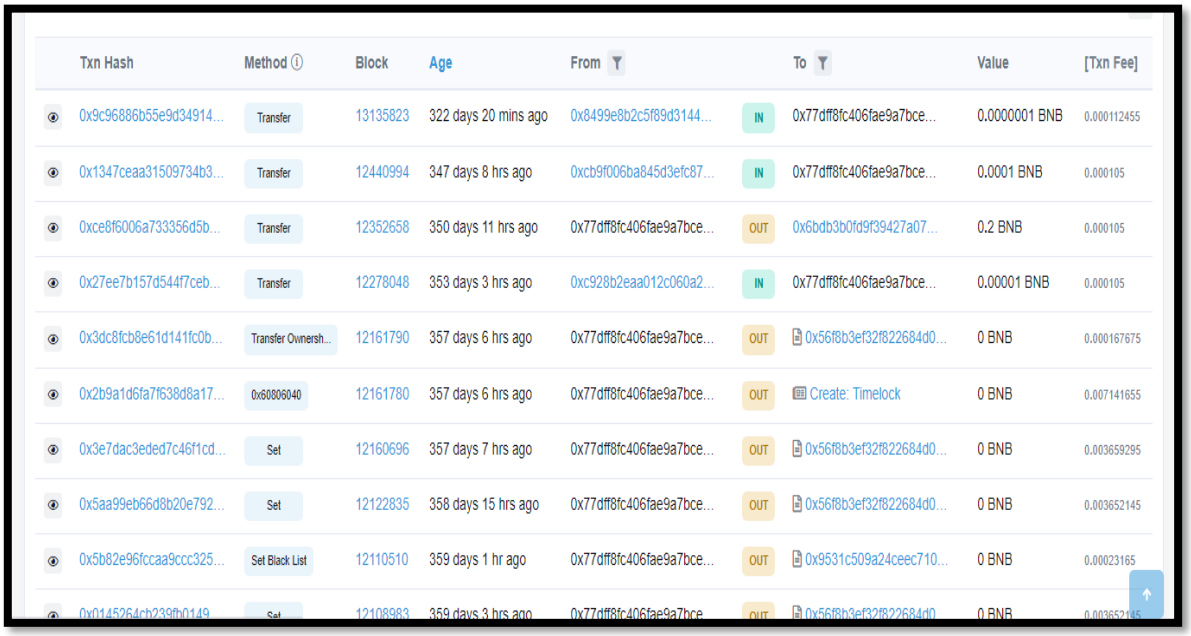


Figure 17: Scope of the Squid Game Scam

In Figure 17 shows the of the Squid Game Token scam that I mapped out by hand showing the connection of each account.

4.2.1 - Creation of Contract

In this section we will show how the author of this scam created the contract and his modus operandi. Before that, let me give you a brief explanation on what's the meaning of each of the fields of the Binance smart chain explorer[5] that through data analytics allows to see what happened inside the blockchain in Figure 18.



Txn Hash	Method	Block	Age	From		To	Value	[Txn Fee]
0x9c96886b55e9d34914...	Transfer	13135823	322 days 20 mins ago	0x8499e8b2c5f89d3144...	IN	0x77dff8fc406fae9a7bce...	0.0000001 BNB	0.000112455
0x1347ceaa31509734b3...	Transfer	12440994	347 days 8 hrs ago	0xcb9f006ba845d3efc87...	IN	0x77dff8fc406fae9a7bce...	0.0001 BNB	0.000105
0xce8f6006a733356d5b...	Transfer	12352658	350 days 11 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x6bdb3b0fd9f39427a07...	0.2 BNB	0.000105
0x27ee7b157d544f7ceb...	Transfer	12278048	353 days 3 hrs ago	0xc928b2eaa012c060a2...	IN	0x77dff8fc406fae9a7bce...	0.00001 BNB	0.000105
0x3dc8fcb8e61d141fc0b...	Transfer Ownersh...	12161790	357 days 6 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x56f8b3ef32f822684d0...	0 BNB	0.000167675
0x2b9a1d6fa7f638d8a17...	0x60806040	12161780	357 days 6 hrs ago	0x77dff8fc406fae9a7bce...	OUT	Create: Timelock	0 BNB	0.007141655
0x3e7dac3eded7c46f1cd...	Set	12160696	357 days 7 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x56f8b3ef32f822684d0...	0 BNB	0.003659295
0x5aa99eb66d8b20e792...	Set	12122835	358 days 15 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x56f8b3ef32f822684d0...	0 BNB	0.003652145
0x5b82e96fccaa9ccc325...	Set Black List	12110510	359 days 1 hr ago	0x77dff8fc406fae9a7bce...	OUT	0x9531c509a24ceec710...	0 BNB	0.00023165
0x0145264cb239fb0149...	Set	12108983	359 days 3 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x56f8b3ef32f822684d0...	0 BNB	0.003652145

Figure 18: Overview of the bscan Fields

- Txn Hash: This field shows us the transaction history registering if the transaction was successful or not, the block in which the transaction was included, the timestamp of a certificate to say at what hour it was done, the From is the person who is sending and the To is the one receiving that transaction, the value of that transaction, the transaction fee is the value to do that transaction and the BNB price is the value that BNB was worth at the time set transaction was done.

[5] https://bscscan.com/

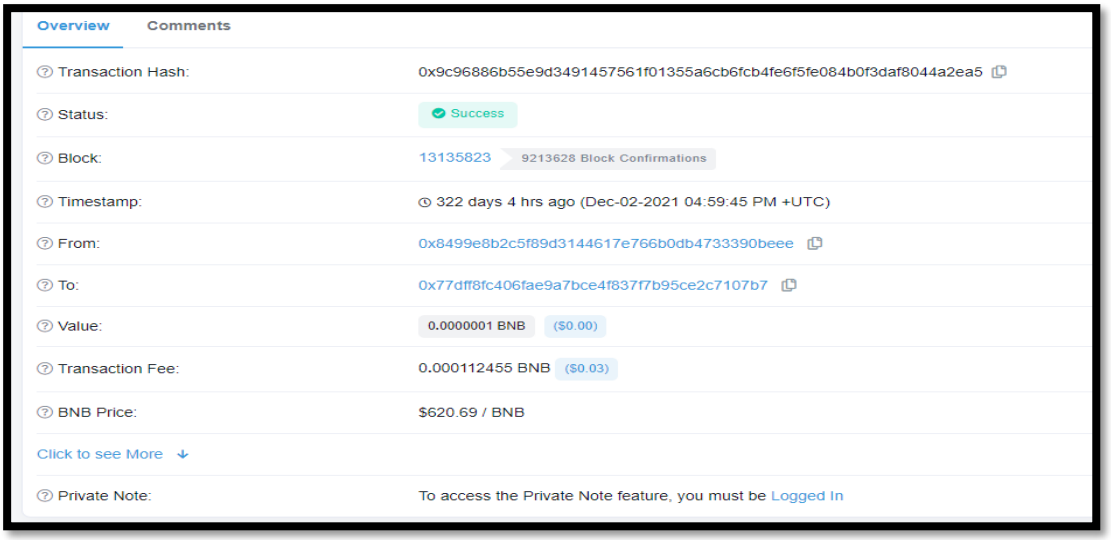


Figure 19: Inside a Txn hash

- Method: The Method are the functions that allow you to create a smart contract or interact with one allowing to transfer your tokens to another wallet or with other tokens. Also, if you create a contract, you can define how other people interacted with that contract. The investors of this scam couldn't sell their Squid Game Tokens because the cybercriminal blacklisted the investors to sell and he was the only person on the whitelist so only he could sell.

- Block: The number of in which the transaction was done on the Binance smart chain.

- Age: The date on when the transactions were done.

- From: The user who is sending to another user.

- To: The user who is receiving from somebody.

- Value: Shows the value in BNB of every individual transaction.

- Txn Fee: Transaction Fee, the cost to do those transactions.

The user 0x77DFf8fC406fAe9A7bCE4F837F7b95cE2c7107b7 started by receiving 1 BNB from the AscendEX Hot Wallet so he would be able to create the contracts since that's the price to create a smart contract in the Binance smart chain. The money came from a hot wallet from an exchange that didn't have KYC (we cannot identify the person because that exchange doesn't collect that information) besides since it came from a hot wallet that's a wallet that exchanges use to send the transactions from users to not be directly linked from that transaction for privacy issues, we can't link it to cybercriminals.

0x60806040	11727023	381 days 22 hrs ago	0x77dff8fc406fae9a7bce...	OUT	Create: SQUID	0 BNB
0x60806040	11727009	381 days 22 hrs ago	0x77dff8fc406fae9a7bce...	OUT	Create: SQUIDToken	0 BNB
Transfer	11726340	381 days 22 hrs ago	AscendEX Hot Wallet	IN	0x77dff8fc406fae9a7bce...	1 BNB

Figure 20: Cybercriminal receives money and creates contracts

After that the cybercriminal created two contracts one was named SQUID with address 0xD103fa462b090eDbD8183E9A8168508e13B2335E initially used for investors to buy the token but in actuality this contract is a honeypot since its actually using the second contract he created SquidToken to do this if we go see the contract source code of SQUID, we can see that there's a SQUID function in there but doesn't do anything the real function behind the source code is the SquidToken.

Contract Source Code Verified (Exact Match)

Contract Name: **SQUID**

Compiler Version **v0.6.12+commit.27d51765**

Contract Source Code (Solidity)

```
1167  // File: contracts/SQUID.sol
1168  pragma solidity 0.6.12;
1169
1170  contract SQUIDToken is ERC20, Ownable {
1171      uint8 private constant DECIMALS = 18;
1172      uint256 private constant INITIAL_TOTAL_SUPPLY = 800 * (10**6) * (10 ** uint256(DECIMALS));
1173
1174      IUniswapV2Router02 public uniswapV2Router;
1175      address public uniswapV2Pair;
1176
1177      function initialize() public initializer {
1178          Ownable.__Ownable_init();
1179          ERC20.__ERC20_init("Squid Game", "SQUID");
1180          _setupDecimals(DECIMALS);
1181          _totalSupply = 0;
1182
1183          _mint(msg.sender, INITIAL_TOTAL_SUPPLY);
1184
1185          uniswapV2Router = IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
1186
1187          // Create a uniswap pair for this new token
1188          uniswapV2Pair = IUniswapV2Factory(uniswapV2Router.factory())
1189              .createPair(address(this), uniswapV2Router.WETH());
1190      }
1191  }
```

Figure 21: SquidToken contract reference

By observing Figure 21 we see that the name of the contract is SQUID but in the source code, we have a function that calls the other contract SQUIDToken that allows the cybercriminal to use the other functions of that contract allowing him to steal the funds using the ApproveTo function we will set implementation from it will upgrade the contract making the code of

SQUIDToken the one it will use.

```
function _approveTo(address newImplementation) internal {
    _setImplementation(newImplementation);
    emit Upgraded(newImplementation);
}
```

Figure 22: Honeypot SQUID Function that upgrades the contract to SquidToken

Method ⓘ	Block	Age	From		To	Value	Txn Fee
Set Illegal List...	11969691	364 days 5 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x87230146e138d3f296...	0 BNB	0.00023187
Set White List	11968968	364 days 6 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x87230146e138d3f296...	0 BNB	0.00023198
Set White List	11968964	364 days 6 hrs ago	0x77dff8fc406fae9a7bce...	OUT	0x87230146e138d3f296...	0 BNB	0.00023198

Figure 23: Methods that blocked investors from selling address SquidToken address 0xD103fa462b090eDbD8183E9A8168508e13B2335E

After that he created the Marbles token address 0x9531c509a24CEEc710529645fc347341FF9F15EA with the same method to steal funds with the SquidToken and finally took out the funds of the 2 tokens stealing around 14 million dollars at the time of the theft.

Contract Name: **Marbles**

Optimization Enabled: **Yes** with **200** runs

Compiler Version **v0.6.12+commit.27d51765**

Other Settings: **default** evmVersion, **MIT** license

Contract Source Code (Solidity)

```
        uint amountIn,
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external;
}

// File: contracts/SQUID.sol
pragma solidity 0.6.12;

contract SQUIDToken is ERC20, Ownable {
    uint8 private constant DECIMALS = 18;
    uint256 private constant INITIAL_TOTAL_SUPPLY = 800 * (10**6) * (10 ** uint256(DECIMALS));

    IUniswapV2Router02 public uniswapV2Router;
    address public uniswapV2Pair;

    function initialize() public initializer {
        Ownable.__Ownable_init();
        ERC20.__ERC20_init("Squid Game", "SQUID");
        _setupDecimals(DECIMALS);
        _totalSupply = 0;
```

Figure 24: Marbles source code

Notice the same pattern the name of the Contract is Marbles but the source code has SQUIDToken and also used of a function to stop people from selling the Marbles token.

Figure 25: Marbles blacklist function stops investors from selling it address 0xD103fa462b090eDbD8183E9A8168508e13B2335E

After a lot of researching, I found the link of how what service the cybercriminals used to make these contracts[6] (the link no longer works) but using the WayBack Machine we can see what it used to look like. This site basically automatically generated the honeypot contracts and you only need to paste de code on the contract and you will be able to do the scam token easily.

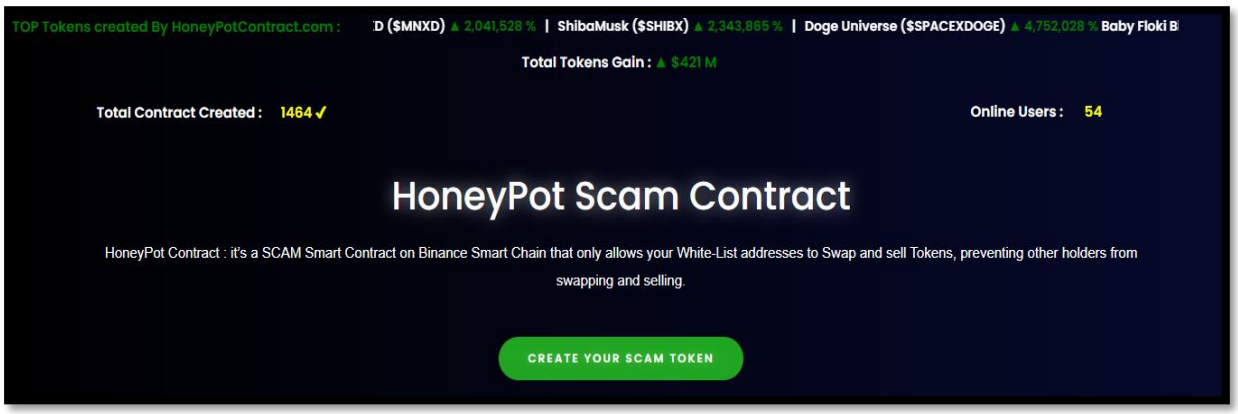


Figure 26: HoneyPot contract generation

4.2.2 - Rugpull and Swapping

In this section we will explain how much money the hacker was able to steal from investors and how the swapping process was in this case trading their currency for BNB. After all these preparations the fund are finally ready to be stolen. The liquidity pool of SQUID was on the address 0x87230146E138d3F296a9a77e497A2A83012e9Bc5 and was sent to 2 different addresses 0x1f5eabba9c56bca4a7828969b79bc87051125b3 named Squid Game Rug 1, they stole around 4 million $ and the second address was 0x34400280a169f4685193926a513618cf7fe7f0aa were they stole 3.37 million $.

[6] https://honeypotcontract.com/

Figure 27: Stolen Amount of Squid Game Rug 1, 4 million $, multiple transactions only showing 1.

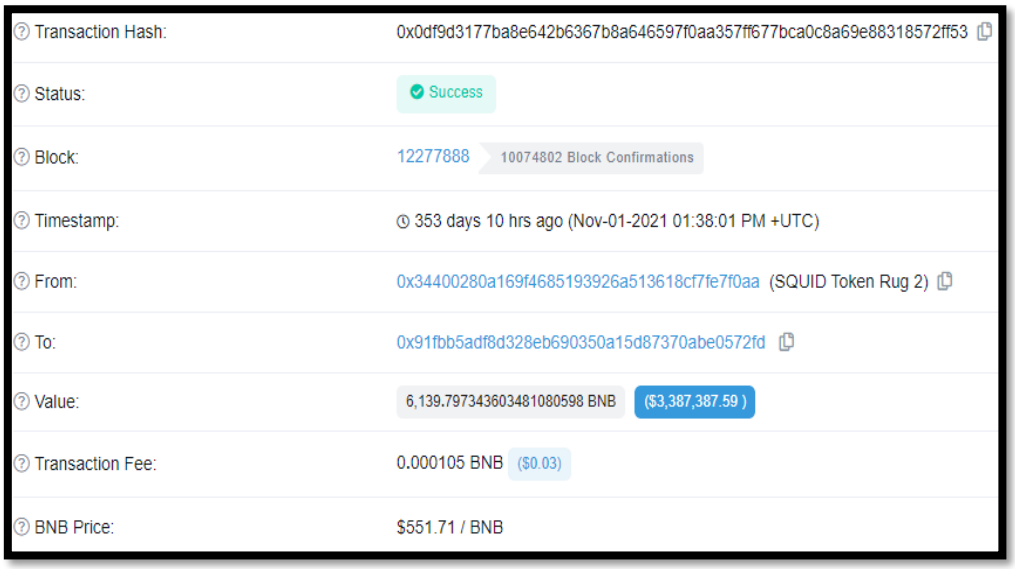


Figure 28: Stolen Amount of Squid Game Rug 2, 3,387 million $

The Marbles token address 0x614826D885FF973324a5C3f43369d7C413a88aea was also stolen for a total amount of 7 million $ at the time of theft from multiple tokens that were staked to earn marble each with different values.

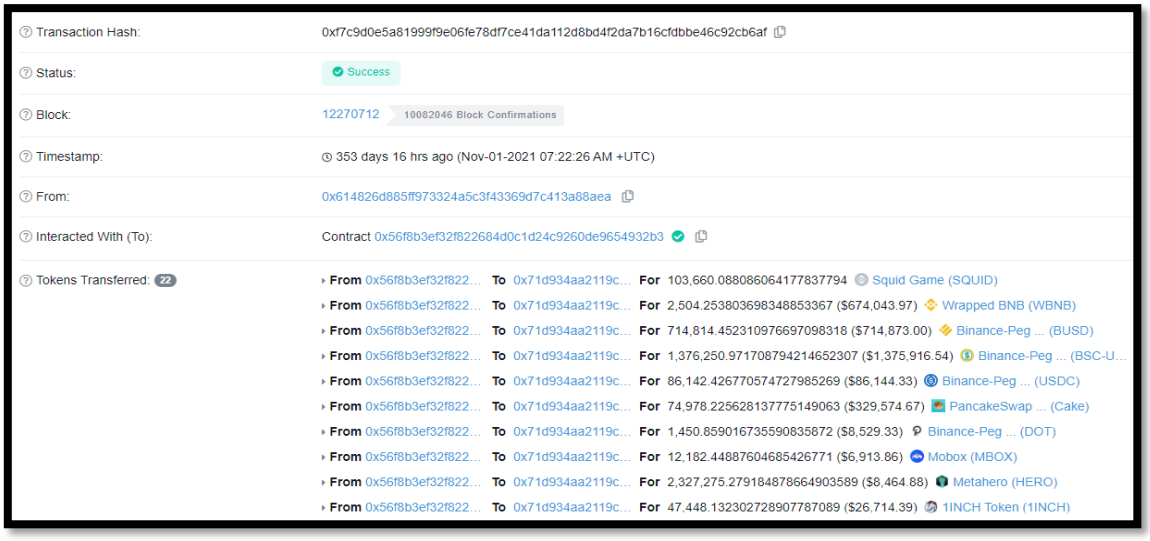


Figure 29: Stolen Amount of the Marble Token, 7 million $

While doing this they converted all the tokens to BNB by swapping the marbles and the SQUID token and now they only need to clean the money using the mixer Tornado.cash.

4.2.3 - Tornado.cash Mixer

In this section we will see how the cybercriminals used the mixer Tornado.cash to clean the money and leave without trail the money was mixed in two different accounts the first one being (0x71d934aa2119ca3995f702f075d540f7a6b0f728) where it cleans the money from SQUID token from the Squid Game Rug 1 and Marbles Token and the second account was (0x91fbb5adf8d328eb690350a15d87370abe0572fdonly) cleans money from Squid Game Rug 2.

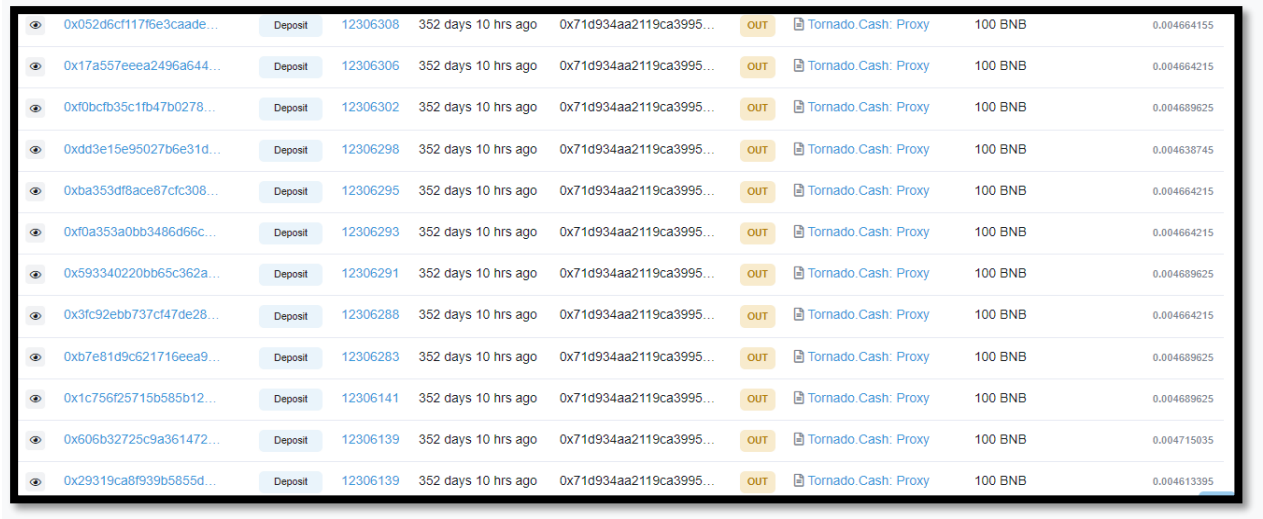
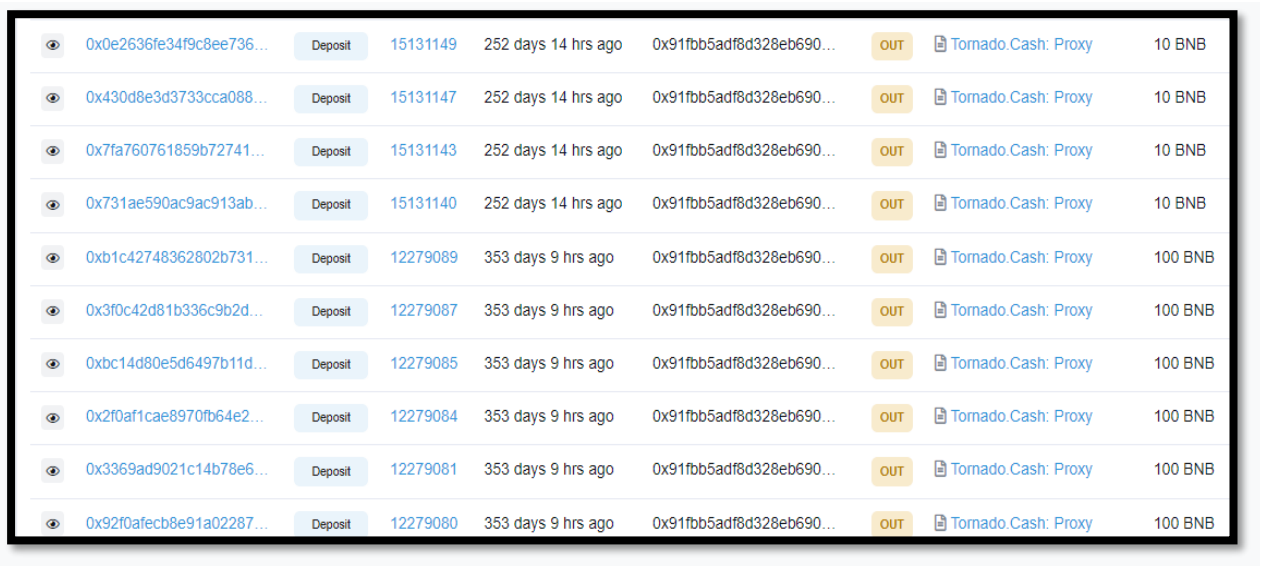


Figure 30: Squid Game Rug 1 and Marbles cleaned on Tornado.cash

As we can see the Cybercriminals sended the money to this account and are now starting to clean it by

sending it to Tornado.cash that's compatible with the BSC sending in 100 BNBs amount to be easier to clean and because it's the max amount Tornado.Cash allows to deposit since if someone would take out a large amount it would be easy to know who it is because only a few amounts of people could take such quantity so by doing it in portions it becomes much harder to do it.



0x0e2636fe34f9c8ee736...	Deposit	15131149	252 days 14 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB
0x430d8e3d3733cca088...	Deposit	15131147	252 days 14 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB
0x7fa760761859b72741...	Deposit	15131143	252 days 14 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB
0x731ae590ac9ac913ab...	Deposit	15131140	252 days 14 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB
0xb1c42748362802b731...	Deposit	12279089	353 days 9 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB
0x3f0c42d81b336c9b2d...	Deposit	12279087	353 days 9 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB
0xbc14d80e5d6497b11d...	Deposit	12279085	353 days 9 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB
0x2f0af1cae8970fb64e2...	Deposit	12279084	353 days 9 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB
0x3369ad9021c14b78e6...	Deposit	12279081	353 days 9 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB
0x92f0afecb8e91a02287...	Deposit	12279080	353 days 9 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB

Figure 31: Squid Game Rug 2 cleaned on Tornado.cash

In this case their cleaning the rest of the money of Squid Game Rug 2 since they don't have left more than 100 BNB after cleaning it multiple times it starts doing it by 10 BNB.

4.2.4 - Conclusion of the Squid Game case

In conclusion about the Squid Game case, they stole around 14 million $ in Section 4.2.2 that was proved by following and providing evidence of their modus operandi in the BSC explorer. Unfortunately we lost their trail since Tornado.cash as mentioned in Section 4.2.3 deletes the trail that connects the user who deposited on the mixer and the wallet who takes out the money from the mixer but we learned how to follow his trail through data analytics showing it us its usefulness of registering all the occurring events that happened in this scam and help us gather evidence in case one day he gets caught bringing out the money out of the blockchain because he only will be able to do this on a place that has some form of KYC and if he cannot explain how he got the money he will most likely get arrested and this evidence used on the court of law since the blockchain is immutable the information can't be forge because the nodes validate each other.

4.3 Liquid Exchange Exploit

In this section we will talk about the Liquid exchange smart contract exploit and how it was done. On August 19th of 2021, [24] this exchange was hacked for a total of 90 million $. The exchange announced the incident through twitter indicating that their hot wallets were compromised. The incident happened because the hot wallet wasn't protected correctly and the hackers got access to it via 3 possible ways, a phishing attack, malware or an inside job making the hackers have access of the wallet and allowing to transfer assets. After that the hacker started to swap the tokens using multiple ways, he sends the money to CEX to take it out which doesn't make much sense unless he managed to fool the KYC system of the Huobi and Bitlaxy since they should have the ID of the hacker behind this. They also used Tornado.cash, in this case, they made a mistake in which they send directly the money to 1 of the wallets that would be used to receive the money from Tornado.cash and we can see what he did after it.

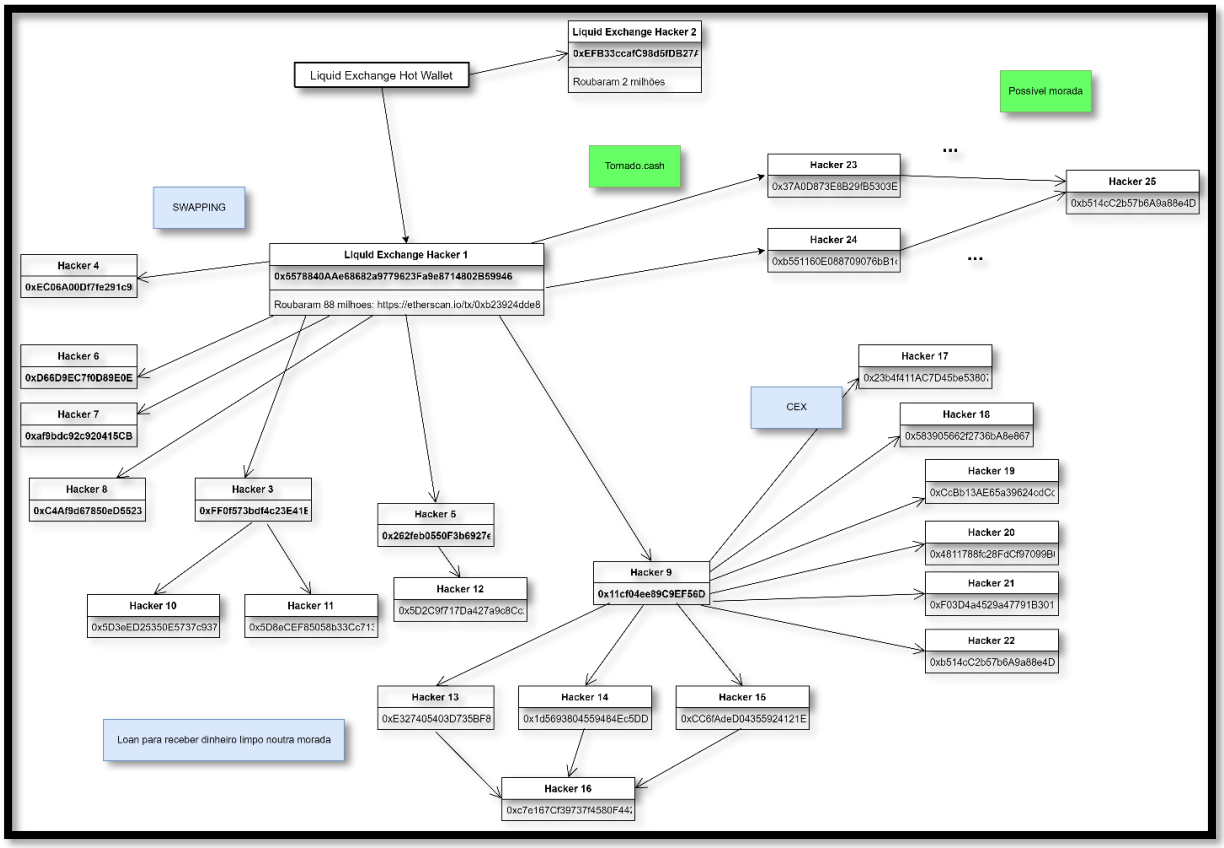


Figure 32: Scope of the Liquid Exchange Hot Wallet Exploit

The only free tool that help us map the blockchain transactions, in this case, the Ethereum blockchain and the name of the tool is Maltego[7]. Maltego is a software that uses multiple libraries for various fields to helps track money laundering and other cybersecurity issues since allows to automatically track the flow inside the blockchain. Using the Tatum library inside Maltego allows to insert an ETH address and

[7] https://www.maltego.com/

search for all the connected accounts to that respective address helping us map out what happen much faster.

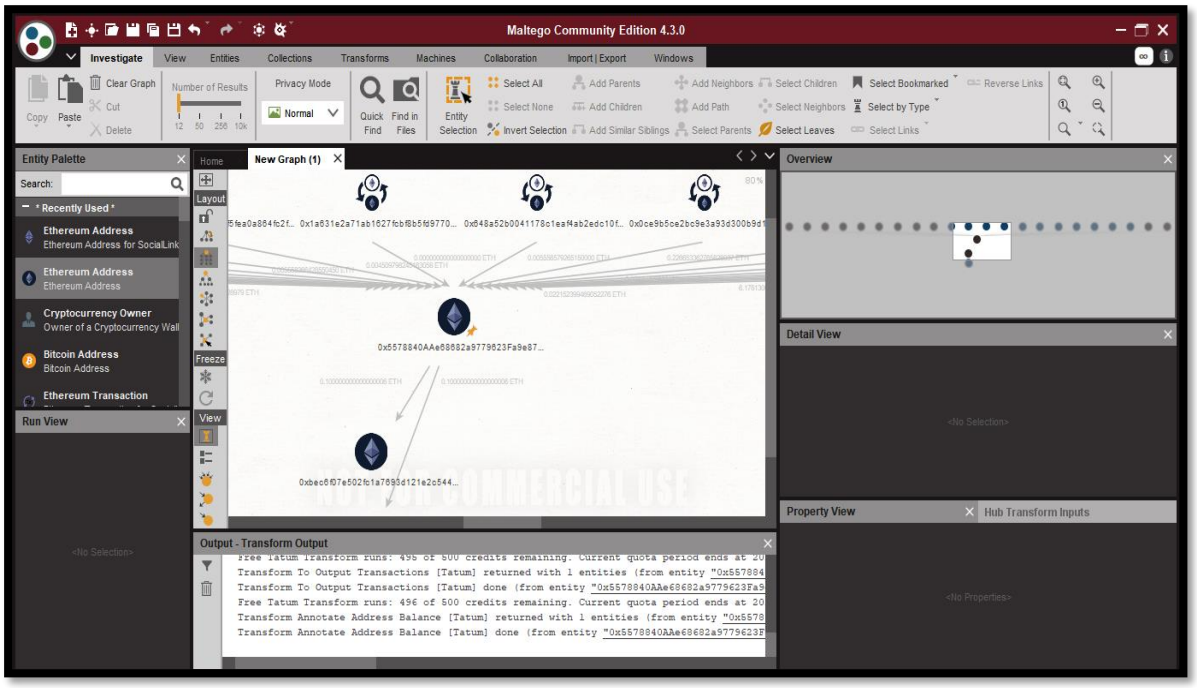


Figure 33: Maltego UI for cryptocurrencies

As you can see in the Figure 33, we inserted in the icon the address that we want to search. We searched address 0x5578840AAe68682a9779623Fa9e8714802B59946 and then we right click the address and run all transforms that function will allows us to see all the inputs and outputs that address did depending on what you want to see. On the Overview tab you got each different address and how it relates with this one making this tool extremely useful in crypto forensic investigation.

To watch what happened in this case we will use the Etherscan [8] that is the same as Binance explorer only it is for transactions on the Ethereum Network since this case was done mainly in there.

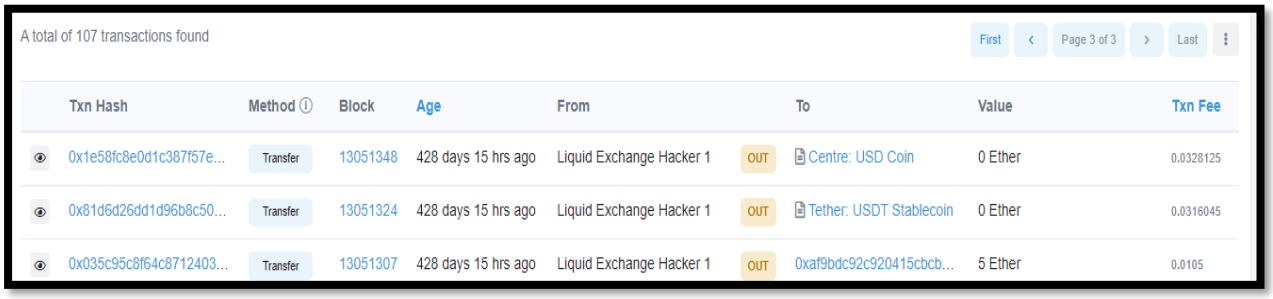


Figure 34: Etherscan.io Interface

As you can see it's the same logic as shown on the Squid Game case, the fields have the same meaning

[8] https://etherscan.io/

as before only now it is on the Ethereum Blockchain network.

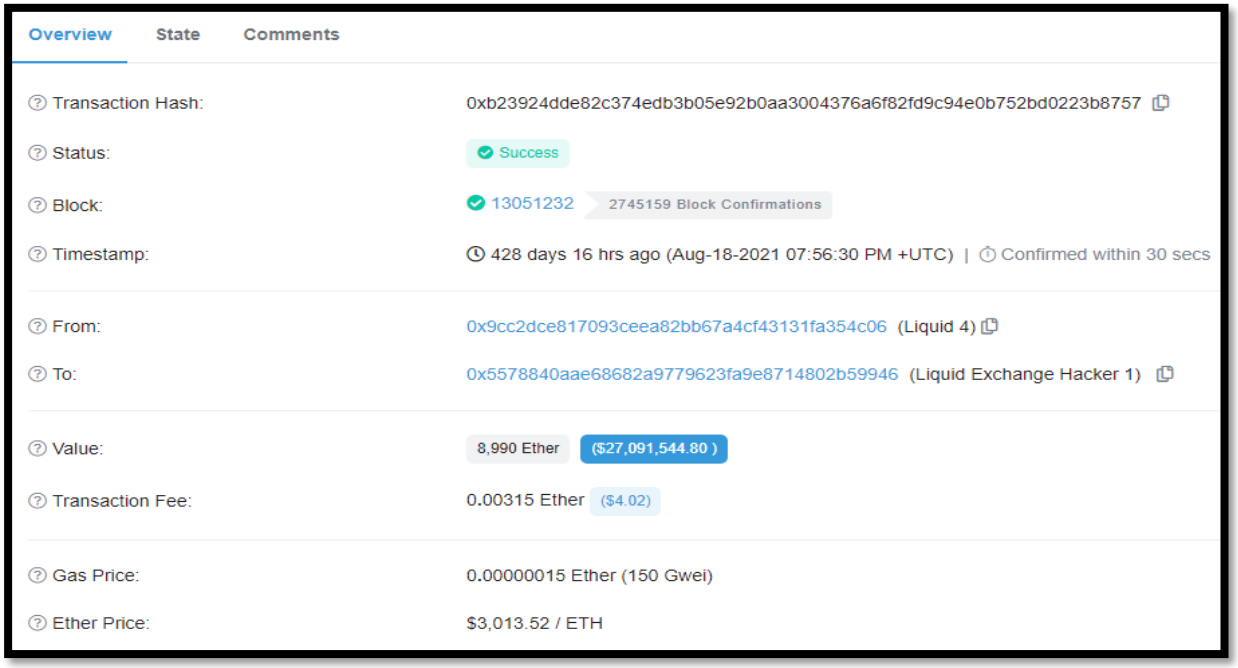
4.3.1 - Hot Wallet exploit

In this section we will see how the cybercriminal exploited 2 wallets those wallets are Liquid 3 0xDb2caD4f306B47C9b35541988c7656F1BB092e15 and the second wallet address Liquid 4 0x9cC2dCe817093CEEa82bb67A4Cf43131fA354c06 and they send their money to the cybercriminal wallet (0x5578840aae68682a9779623fa9e8714802b59946).

0x5baf1208cf1bd153322...	Transfer	13051240	428 days 15 hrs ago	0xd0b8414caba5228716...	IN	Liquid Exchange Hacker 1	272.057698451 Ether
0xe9e5460cca6810a4eb...	Transfer	13051239	428 days 15 hrs ago	0xb478c93509ecba29f7...	IN	Liquid Exchange Hacker 1	505.419567549805647 Ether
0x05dd45f14b898ab247...	Transfer	13051235	428 days 15 hrs ago	Liquid 3	IN	Liquid Exchange Hacker 1	530 Ether
0xb23924dde82c374edb...	Transfer	13051232	428 days 15 hrs ago	Liquid 4	IN	Liquid Exchange Hacker 1	8,990 Ether

Figure 35: Hacker sending funds to his wallet

The total amount stolen from the two hot wallets amounts to 90$ million at the time of transaction and the cybercriminal starts swapping the other tokens it stole to ETH in multiple different wallets to me easier to clean the money on the mixer and in this case other platforms.



Overview | State | Comments

Transaction Hash:	0xb23924dde82c374edb3b05e92b0aa3004376a6f82fd9c94e0b752bd0223b8757
Status:	Success
Block:	13051232 2745159 Block Confirmations
Timestamp:	428 days 16 hrs ago (Aug-18-2021 07:56:30 PM +UTC) | Confirmed within 30 secs
From:	0x9cc2dce817093ceea82bb67a4cf43131fa354c06 (Liquid 4)
To:	0x5578840aae68682a9779623fa9e8714802b59946 (Liquid Exchange Hacker 1)
Value:	8,990 Ether ($27,091,544.80)
Transaction Fee:	0.00315 Ether ($4.02)
Gas Price:	0.00000015 Ether (150 Gwei)
Ether Price:	$3,013.52 / ETH

Figure 36: 27$ million stolen on a single transaction

4.3.2 - Swapping

In this section we will talk how the hacker starts sending money to multiple addresses to swap the tokens and send to the original address for then send for other addresses for mixing purposes or cashing out. Hacker 3 to Hacker 9 swap wallets to trade the tokens, Hacker 11 to 15 are wallets that he left some money behind so in the future the hacker comes back to clean the rest of the money, and the other wallets where the tokens have passed are used to confuse the trail to follow the money and wallets from Hacker 16 to Hacker 25 are for mixing or cash out purposes to get away with the stolen funds.

0x3242c23086d14c1480...	Multicall	13051739	428 days 16 hrs ago	0xec06a00df7fe291c9f8...	OUT	Uniswap V3: Router	0 Ether
0xe58fdb4b191bc48aa5...	Multicall	13051707	428 days 16 hrs ago	0xec06a00df7fe291c9f8...	OUT	Uniswap V3: Router	0 Ether
0xb161e21fd62904990d...	Multicall	13051664	428 days 16 hrs ago	0xec06a00df7fe291c9f8...	OUT	Uniswap V3: Router	0 Ether
0xa12fdb21297fa3148bf...	Multicall	13051619	428 days 16 hrs ago	0xec06a00df7fe291c9f8...	OUT	Uniswap V3: Router	0 Ether
0x49e973cba88162ebca...	Multicall	13051588	428 days 17 hrs ago	0xec06a00df7fe291c9f8...	OUT	Uniswap V3: Router	0 Ether
0x2c783de5483af680c4f...	Multicall	13051581	428 days 17 hrs ago	0xec06a00df7fe291c9f8...	OUT	Uniswap V3: Router	0 Ether

Figure 37: Swapping tokens on Uniswap for ETH Hacker 4 wallet (0xEC06A00Df7fe291c9F872449385BD593E38d8133)

The cybercriminal started swapping the money on a DEX named Uniswap and did the same process that I have shown on the Squid Game case that the hacker swap BNB tokens for SQUID on another DEX Pancakeswap. But in this case its Swapping other stolen tokens for Ethereum to send it to the mixer.

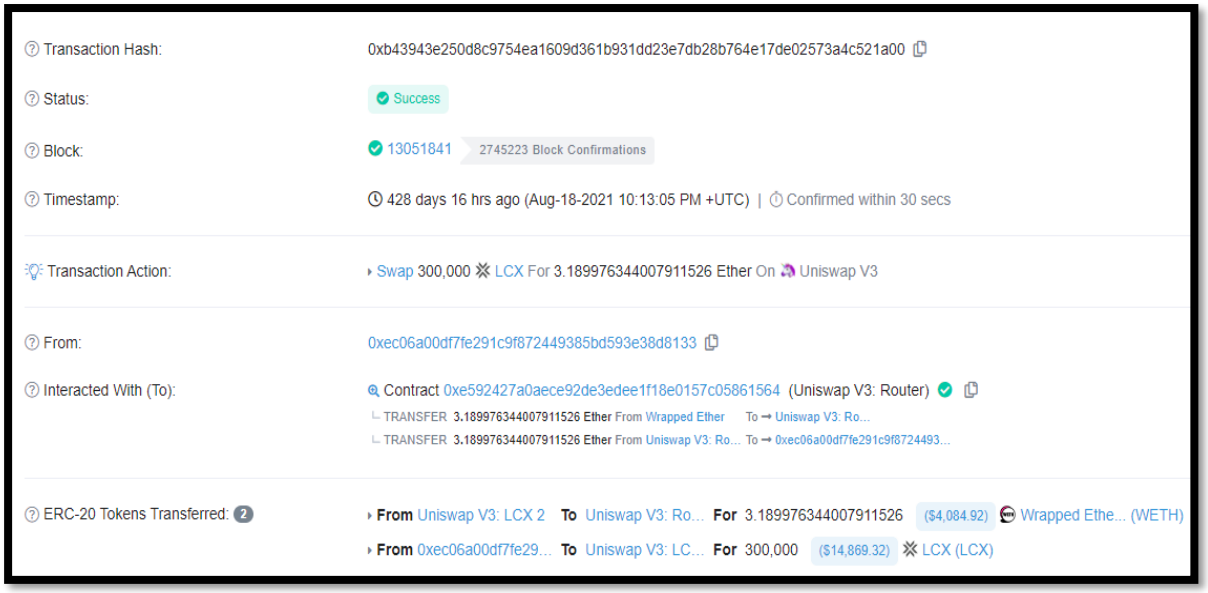


Figure 38: Inside a Swapping transaction LCX for Wrapped ETH

We can see that the hacker is trading LCX for Wrapped Ethereum. In case you didn't know wrapped

ETH is a derivate that mimics the price of ETH these kinds of tokens were created to be used on a different blockchains because for example bitcoin can't be used directly on the Ethereum blockchain since it doesn't support smart contracts so Ethereum created a derivate named wrapped Bitcoin that mimics the price of Bitcoin to be used instead and hackers use this in case they want to send the money to a different blockchain which will show at the next section where the hacker changes the money to the bitcoin blockchain.

4.3.3 - Tornado.cash Mixer and CEX cashout

In this section we observe that the cybercriminals not only used Tornado.Cash but other services to disperse the money. The first one was CEX Hacker 17 to Hacker 21 send the money to exchanges Huobi and Bilaxy. With KYC that should be able to identify him unless it's the wallet of a random person to distract us of catching is trail or he somehow manage to fake an ID and the KYC accepted his account.

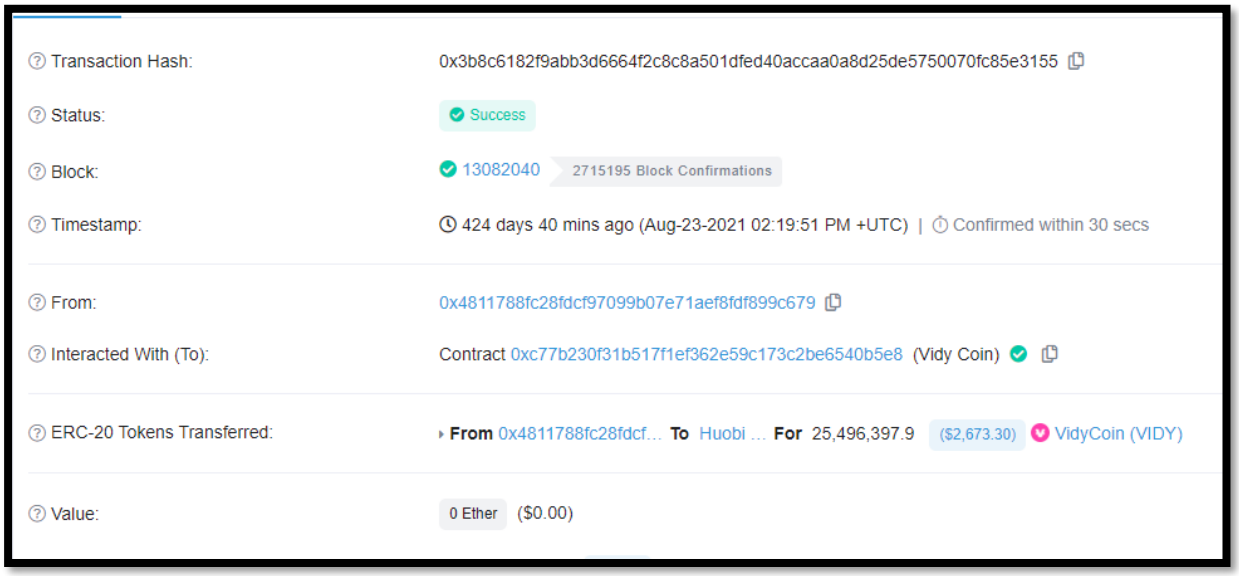


Figure 39: Hacker sending money to Huobi Hacker 20 (0x4811788fc28FdCf97099B07E71aef8Fdf899c679)

We can see that the hacker sends VIDY coin to the Huobi wallet that at the time of theft was worth 60 $ thousand.

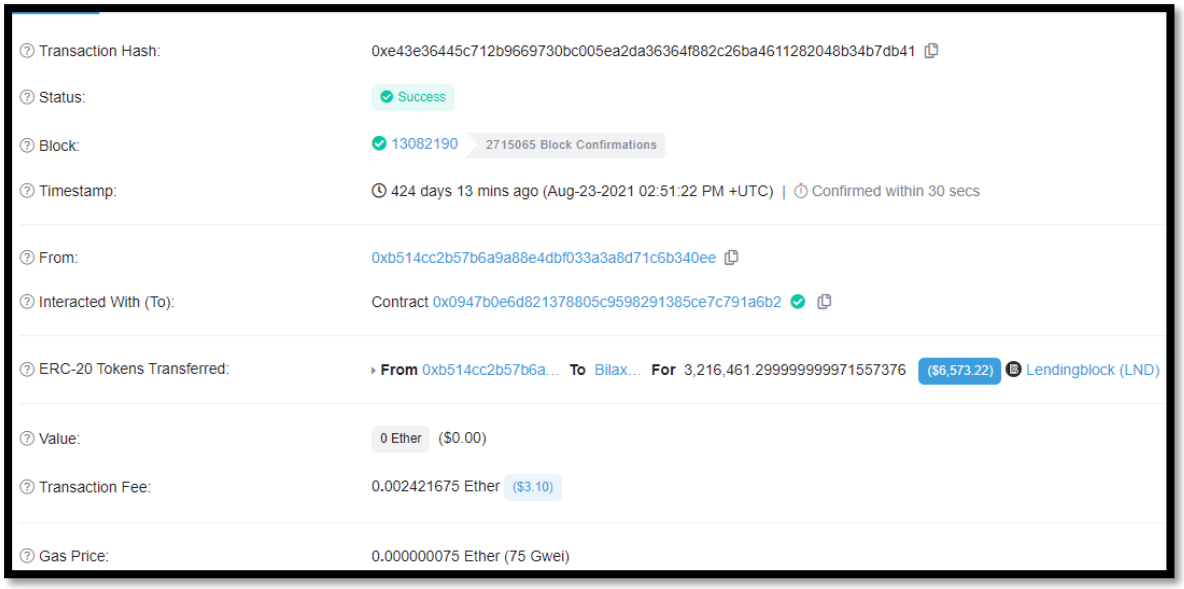


Figure 40: Hacker sending money to Bilaxy Hacker 22 (0xb514cC2b57b6A9a88e4DBf033a3A8d71c6b340eE)

We can see that the hacker sends LND coin to the Bilaxy wallet that at the time of theft was worth 6.5 $ thousand.

The rest as usual was through the Tornado.cash mixing service Hacker 23 address 0x37A0D873E8B29fB5303E00e9300Ccb2EeB5A2786 and then in the Hacker24 address wallet 0xb551160E088709076bB1c25A33028c040e790f61 started to launder the money and made us lose track of the transaction flow after the mixer.

Figure 41: Money laundering Tornado.cash Hacker 23 wallet (0x37A0D873E8B29fB5303E00e9300Ccb2EeB5A2786)

They start to launder 100 ETH per transaction the usefulness of Tornado.cash for cybercriminals is that allows to interact to clean money with multiple different blockchains in the squid game case that we analysed they were laundering BNB and in this one they are laundering ETH.

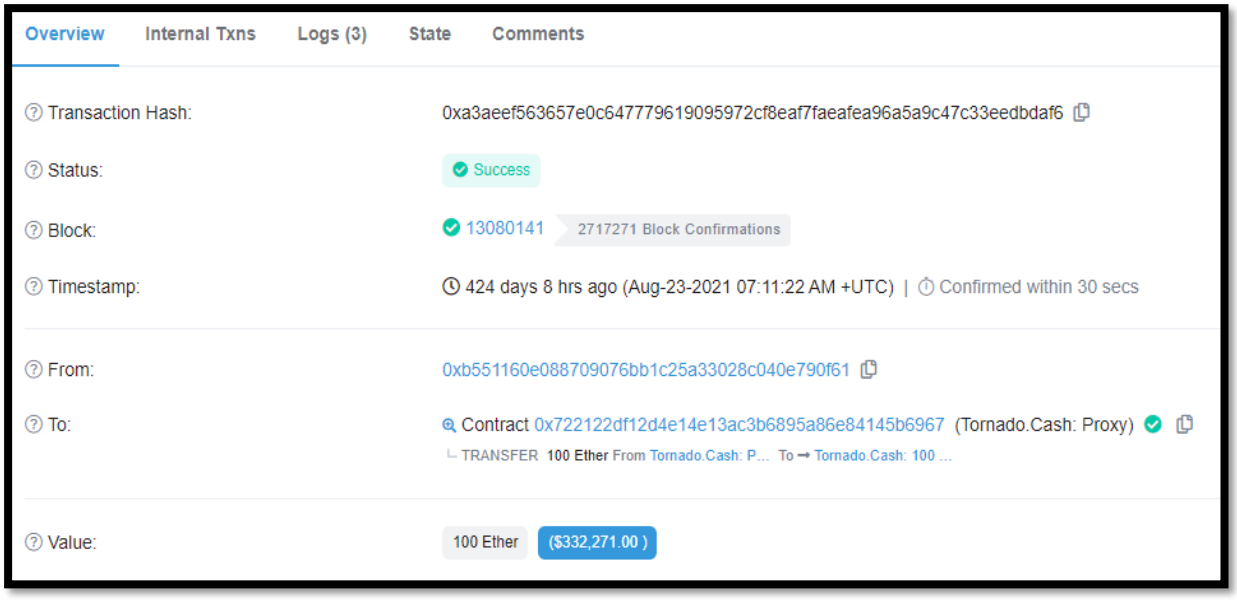


Figure 42: Hacker 24 laundering money on Tornado.Cash value of transaction

This is what it looks like inside a Txn hash to Tornado.Cash stealing with this single transaction around 332 $ thousand and interacting with the proxy contract that doesn't allows us to continue the flow of money.

4.3.4 - Hackers Mistake

In this section we will see how the hacker made a mistake. If we go look at the Hacker 24 Wallet 0xb551160E088709076bB1c25A33028c040e790f61 that was used for laundering we can see that it sent money to a different address and if we follow the flow of transactions of those addresses.

We can see that the last address receives from 3 other addresses that received money from Tornado.cash so we initially assume it's from the same person because its unlikely that its from a random user because these addresses do a transaction to the same end wallet where then it changes to the bitcoin blockchain to run with the money.

Figure 43: Hackers mistake that made us connect the wallets

We can Observe that at the Hacker 24 Wallet (0xb551160E088709076bB1c25A33028c040e790f61) he

made a mistake on the first line he sends the rest of the Ethereum to another wallet instead to Tornado.cash making us be able to chase the trail.

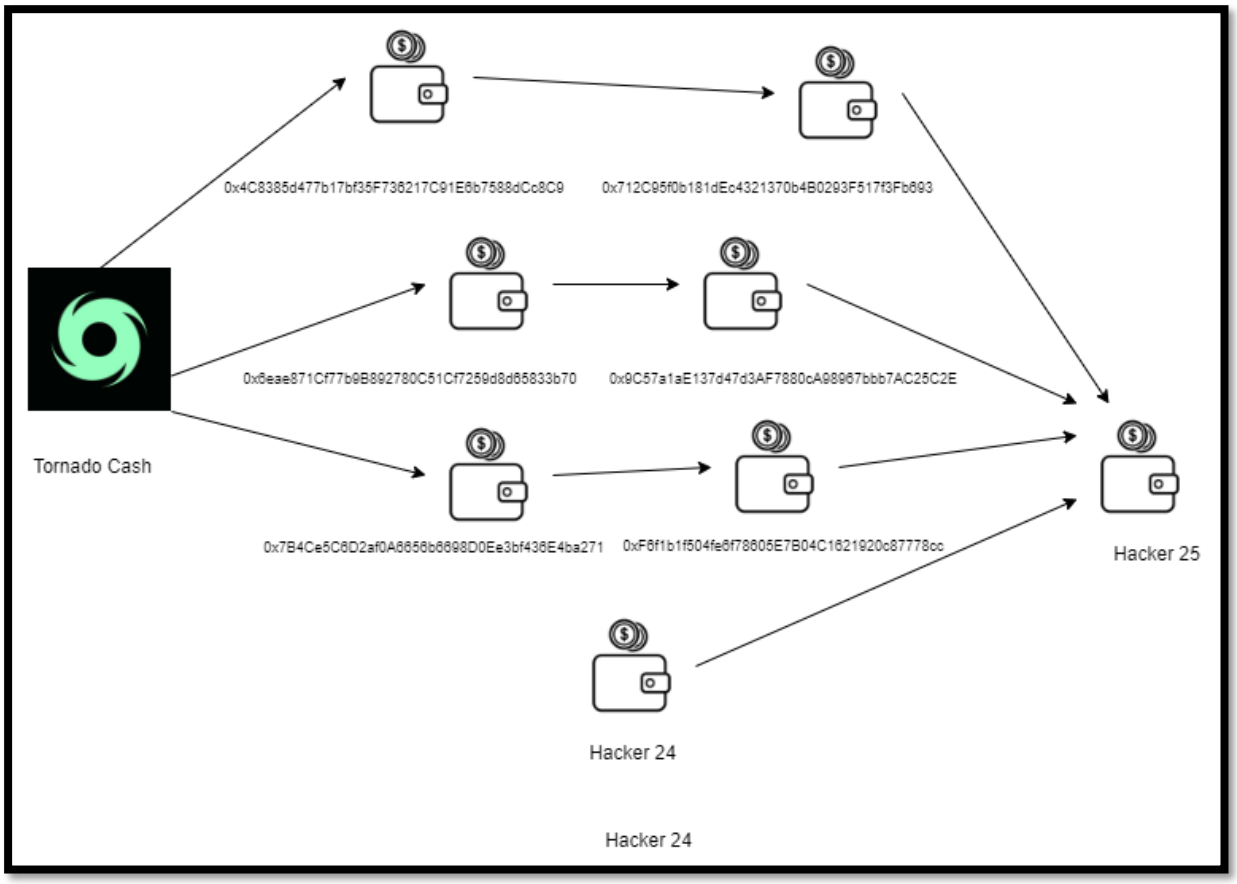


Figure 44: Following the Mistake of the hacker

In Figure 44 we can observe the transaction flow that occurred watching that 3 wallets sent money to Hacker 25 address 0xC4C6E460D0F659e99802208813A2Cc80a0F8B7Fe after receiving it from Tornado.cash making me believe with confidence that the hacker is linked with these accounts. First let's see what is liked to receive a transaction from Tornado.cash to understand easily why we normally can't track the money.

Method	Block	Age	From		To	Value
Transfer	13080181	432 days 19 hrs ago	0x4c8385d477b17bf35f7...	OUT	0x712c95f0b181dec432...	499.7651 Ether

Figure 45: Wallet that received from Tornado.Cash

As you can see the wallet receive from Tornado.Cash but doesn't show that Tornado sent to this address making connecting both accounts nearly impossible even looking inside the Txn Hash we can not find any clue to link us to that service.

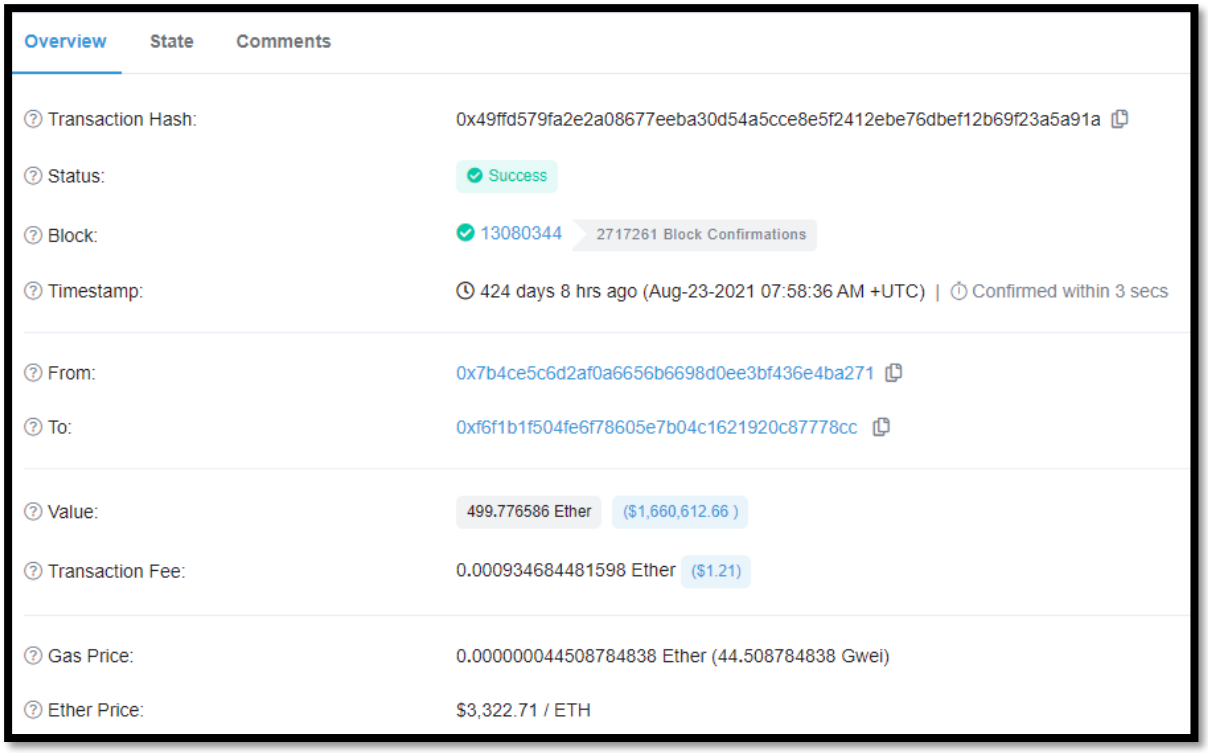


Figure 46: Txn from Tornado.cash

Looking at the Txn we can know that this user received 1.6 $ million in ETH but doesn't tell us where it came from. The from address that is shown on Figure 46 is the address of this wallet and not the Tornado.cash relay that send it here. We could look on the Tornado Cash Contract to see which was the transaction of the Tornado Proxy but it would take too much time and be nearly impossible to find it because that contract does dozens of transactions per day.

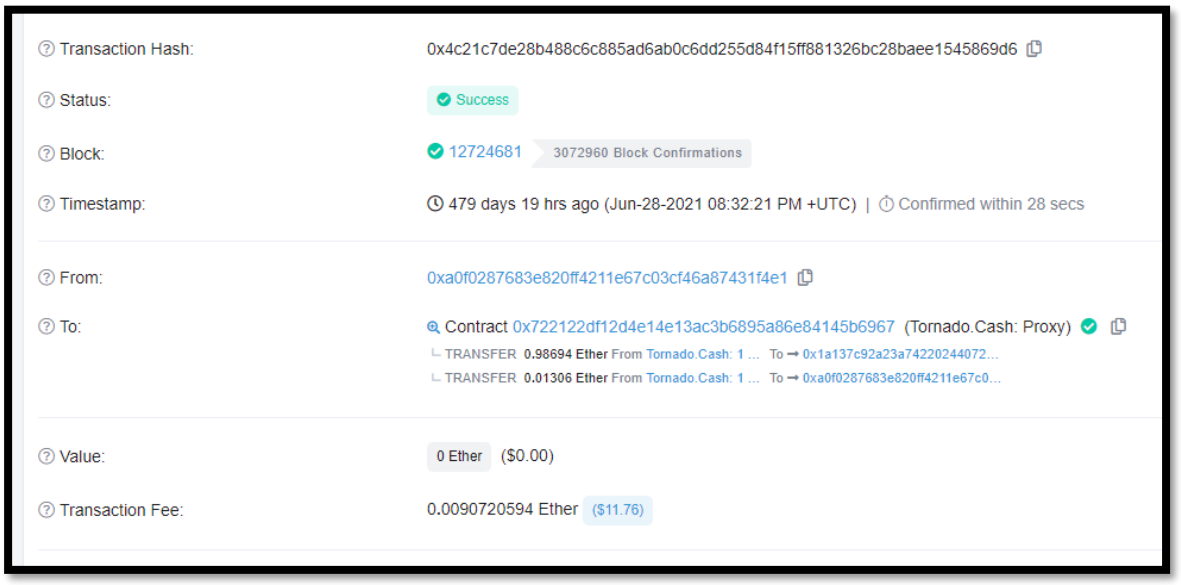
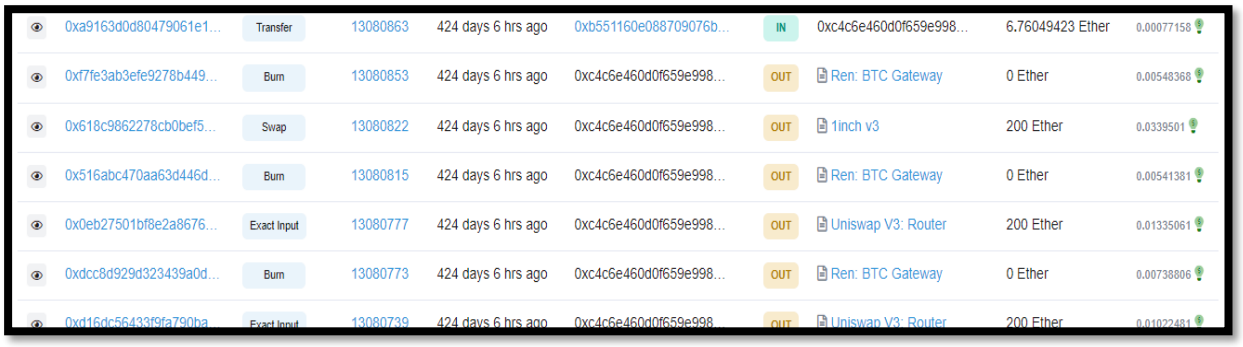


Figure 47: Example of a Tornado Proxy deposit transaction

We would have to search one by one until we find the correct transaction and even if we had found it

would only tell us that it came from Tornado Cash making it tracking it nearly impossible.



0xa9163d0d80479061e1...	Transfer	13080863	424 days 6 hrs ago	0xb551160e088709076b...	IN	0xc4c6e460d0f659e998...	6.76049423 Ether	0.00077158
0xf7fe3ab3efe9278b449...	Burn	13080853	424 days 6 hrs ago	0xc4c6e460d0f659e998...	OUT	Ren: BTC Gateway	0 Ether	0.00548368
0x618c9862278cb0bef5...	Swap	13080822	424 days 6 hrs ago	0xc4c6e460d0f659e998...	OUT	1inch v3	200 Ether	0.0339501
0x516abc470aa63d446d...	Burn	13080815	424 days 6 hrs ago	0xc4c6e460d0f659e998...	OUT	Ren: BTC Gateway	0 Ether	0.00541381
0x0eb27501bf8e2a8676...	Exact Input	13080777	424 days 6 hrs ago	0xc4c6e460d0f659e998...	OUT	Uniswap V3: Router	200 Ether	0.01335061
0xdcc8d929d323439a0d...	Burn	13080773	424 days 6 hrs ago	0xc4c6e460d0f659e998...	OUT	Ren: BTC Gateway	0 Ether	0.00738806
0xd16dc56433f9fa790ba...	Exact Input	13080739	424 days 6 hrs ago	0xc4c6e460d0f659e998...	OUT	Uniswap V3: Router	200 Ether	0.01022481

Figure 48: Hacker 25 Wallet swapping and sending money to Ren Btc

The hacker at the final wallet proceeds to swap the money on Uniswap again and converts the tokens to wrapped BTC (WBTC) and proceed to convert them to RenBtc[9] to use the Ren Btc gateway to send the RenBtc to the BTC blockchain. Ren is a protocol created on Ethereum that creates tokens that mimic the behaviour of other assets like BTC or Ethereum to be able to cross-chain and ren provides the liquidity to make that happen.

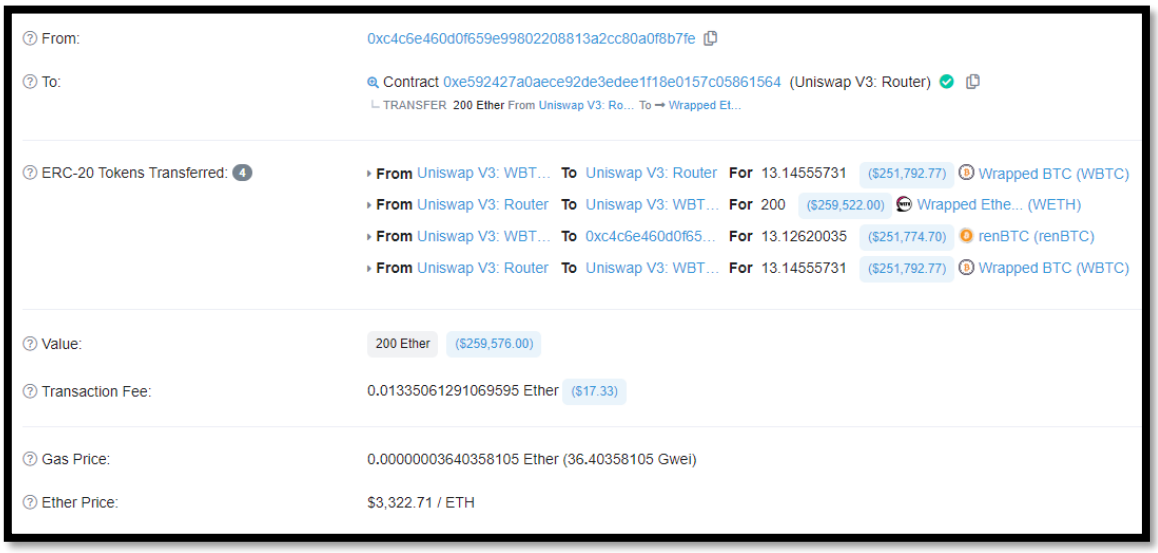


Figure 49: Swapping money for RenBTC to send to the Bitcoin Blockchain

RenBTC also won't allow us to see to which address the money went the difference with Tornado.Cash is that the hacker can't take it whenever he wants since he's just sending the money to other blockchain and not holding it for a while and then taking it out. The only way to find it is by trial and error to find between the days he sent the money in this case 23 August of 2021 on the bitcoin blockchain and find matching transactions with the amount he sent.

[9] https://renproject.io/

Figure 50: Hackers Wallet on the Bitcoin Network

After trial and error, we found 3 wallets that might belong to the hacker in Figure 50 we can see the last transaction of a wallet that hasn't moved since 2021 (16EjYD8gUJLAUvgzRhU9uwFh9zq1efLpzm) to see this transaction we used the Blockchain Explorer [10] and search the address showing us his activity on this network. The other 2 addresses are (15vp5bKz2HEyXozaj1Qj5bvErGmEHDJRnj) and (15hGxz64gCPfUiLKbH7CTgGbk7wNKQw89G) and also haven't moved since 2021 making me believe that these are the accounts the hacker left part of the money and is waiting for 1 day to come back and get it.

We can confirm that the hacker is still active till this day since the Hackers wallet 2 had some movement recently in the last 3 months washing some money he left behind on that wallet.

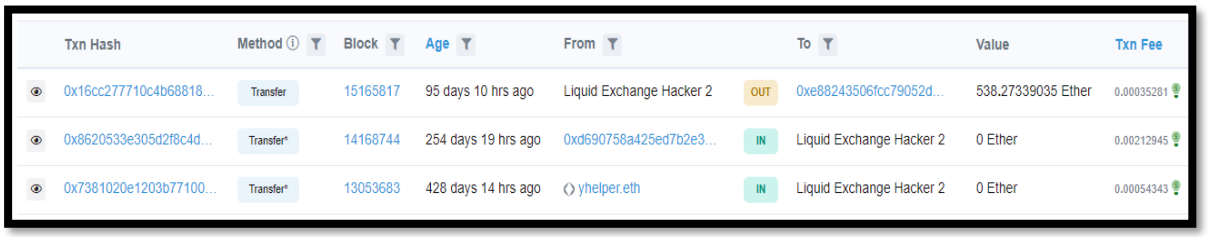


Figure 51: Hackers 2 Wallet (0xefb33ccafc98d5fdb27a6f5ff17350ca76bf3b53) movement after 1 year inactive.

After 1 year has passed, he comes back to get more money that he left behind in the Hacker wallet 2 nearly 2.3 $ million at the time of theft and proceeds to wash it on Tornado.Cash.

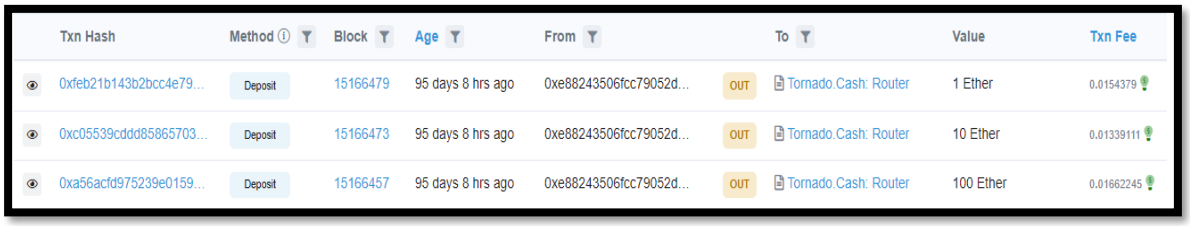


Figure 52: Hacker's wallet 26 (0xE88243506FCc79052d85ad449eF6A02ACE51c3c6) Money laundering

[10] https://www.blockchain.com/explorer

4.3.5 - Conclusion of the Liquid exchange Scheme

In this section we can conclude after extensive investigation we found out how the cybercriminal money launder the 90 $ million that it stole from this Japanese exchange trying to confuse by swapping the money on a lot of different wallets to make us lose track and guide us to dead ends which is the more likely in the CEX to distract us to caught him. He made a mistake at the time he tried to launder the money which led us to 3 of his wallets that he uses to store some of his assets that are worth 100 BTC that at time of writing this is worth 2 $ million. His highly likely that he still has more wallets but we haven't found them yet and we proved also he is still active roaming around searching for more exploits to steal more money. Eventually he should get caught since his greed knows no limits since he continues to be active even after stealing 90 million, we should hear about it in a couple of years.

4.4 - Comparison Between the Squid Game Case and the Liquid Exchange Case

Comparison	Scam Token	Wallet Exploit	Stolen funds	Swapping	Tornado.Cash
SQUID	X		14 million $	X	X
Liquid Exchange		X	90 million $	X	X

Table 1: Comparison between Squid Game and Liquid Exchange

In this section we analyse these two cases and in comparison, we can see that even though the methods on how this scam started in different ways the process in which they try to launder the money is the same. Swapping the tokens stolen from investors by exploiting the smart contracts to make the cybercriminals able to steal the funds from the investors and then proceed to mix the money to erase the trail they left behind using Tornado.Cash and in the future cybercriminals will probably use some mixing tool even more advanced than this one making it even harder to find them. In the Squid Game Token case they got away with 14 million dollars and on the Liquid Exchange case they stole around 90 million $. We can observe that exchanges are the highest target for exploits for the huge potential of profits in they manage to exploit their smart contract and obtain their funds and get away with them. With this comparison we were capable to create a good methodology on how to gather evidence on an efficient matter on decentralized finance exploits and scams, the blockchain since its immutable makes this evidence unforgeable and provides us with high detail on how every transaction was done inside it through the power of data analytics. With this we created a forensic model that can be used on the future

to gather this evidence.

4.5 - Evaluation

In this section we will evaluate the methodology that we elaborated to develop the tool CoinFetch and the framework to be able to analyse cryptocurrency scams on the BSC and Ethereum networks and smart contract exploits followed by the results of the proposed solutions I developed.

4.5.1 – Methodology

In this section we will see the methodology that was used to elaborate the CoinFetch tool and the framework to analyse cryptocurrency scams and exploits on smart contracts. CoinFetch was elaborated in node.js using React to have a clean and simple user interface. The software connects with two different API end points that are CoinGecko and Go + security. We use the CoinGecko API to obtain data about cryptocurrency projects that are gathered in the CoinGecko repository providing us with clean data about the overall information of the project Section 4.1.2. The second API is Go + Security that is an API that allows us to do smart contract audits by using the information that CoinGecko provides us about the contract address and verify if that address its safe for use or it can be exploitable Section 4.1.3.

The framework that we elaborated to analyse cryptocurrency scams consists in three phases: Find the scam token developer address or the first transaction after an exploit of a hot wallet to find the initial flow the transactions Section 4.2.1. The second phase consists in documenting the swapping transactions with their respective wallets to able to trace the money flow inside the blockchain Section 4.2.2. Finally, the last phase is finding the cryptocurrency mixer wallets that should be at the end of the transaction flow when the hackers deposit the money inside the mixer making us lose their trail Section 4.2.3.

4.5.2 - Results Analysis

In this section we will talk about the results of my proposed solutions. The first one was managing elaborated a tool that was able to gather information from a project in the BSC or ETH network to provide us with the overall scope of what that project consists Section 4.1.2 and provide a solution to be able to audit smart contracts on those networks to see if the contract has any vulnerabilities that can be exploited to steal the funds from crypto users Section 4.1.3 guarantying with this the safety of the individual that uses the CoinFetch tool if he chooses to use those smart contracts. The second solution I provided was creating a simple framework that helps people with no prior crypto forensic research understand in a simple manner how those cybercriminals operate in the blockchain network and how to track their crypto transaction flow with no additional tool.

4.6 - Summary

This section started by giving an overview about the CoinFetch tool and its applications in Section 4.1 to Section 4.1.3 to gather information of the requested projects through the CoinGecko API. Followed by Section 4.2 to Section 4.2.4 where we explain the framework on how we start to find the wallet that created the honeypot contract followed by identifying the wallets he used to swap the money and finally using a mixer to clear the trail of the hacker in the BSC network. Followed by Section 4.3 to Section 4.3.5 where we analyse an exchange hot wallet exploit and show the framework on how to analyse a hot wallet exploit tracing the wallets that were used to swap the currency and how they sent the money to the mixer, we even were able find where the hacker has left part of the money and their respective addresses. Followed by Section 4.4 we made a comparison between these two cases and the lessons learned from them. Finally, we conclude with Section 4.5 to 4.5.2 to explain the methodology to elaborate the CoinFetch tool and the results that we got from it.

Chapter 5

5 - Conclusions

With this work were able to analyse how decentralized finance works and provide a methodology to analyse these scams and exploits in a pretty efficient matter providing clear examples, step by step on how everything works since how would an investor buy these tokens to then the cybercriminals start using their modus operandi to swap the tokens after exploiting the smart contract for their benefit either by creating a honeypot contract or through malware/phishing to obtain the credentials to an exchange hot wallet to steal their funds .To then learned how a mixer works and how the cybercriminals send the investors funds to it to clear evidence that links them to that stolen money using Tornado.cash. Even if the U. S Treasury took down the Tornado.cash website its contract its still on the blockchain to be used and even if they don't use it, they still have other mixer alternatives has good as this one like Monero. The only solution that I can provide to avoid cybercriminals launder money is make a watchlist of all the wallets that used a mixer and if they aren't able to justify where did those funds came from its highly likely they were stolen even though the use of a mixer is not illegal this is the only way I can imagine to keep safe the assets of stolen investors. So, the methodology it's still the same but the medium in which is done may differ but with this work we were able to learn how to use the power of data analytics to analyse in a forensic matter the blockchain and help guide people understand how to do a forensic investigation in this matter.

5.1 - Future Work

With this work we provided a useful tool for gathering the overall crypto information of these projects followed by the smart contract audit that can be done on them to see if they are safe. We also provided a framework on how to forensic analyse these projects Section 4, an improvement that can be made in the future on the CoinFetch program is using an API that automatically follows all the transaction flows of those wallets to have an overall view the entire crypto flow of those wallets without doing it manually and maybe even create a program to catch unusual transaction sizes inside a blockchain that might be related to money laundering. Nonetheless, we were able to create a tool that could help thousands of crypto users verify if their investments are safe and created a framework to learn on how to forensically analyse the BSC and ETH blockchain.

6 - References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://www.debr.io/article/21260.pdf. [Accessed 13 December 2021].

[2] M. D. Pierro, “What Is the Blockchain?,” *in Computing in Science & Engineering,* vol. 19, no. 2017, pp. 92-95, September/October 2017.

[3] Fergal Reid, Martin Harrigan, “An Analysis of Anonymity in the Bitcoin System,” 22 June 2011. [Online]. Available: https://arxiv.org/pdf/1107.4524.pdf. [Accessed 5 March 2022].

[4] D. G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” 2017. [Online]. Available: https://gavwood.com/paper.pdf. [Accessed 25 January 2022].

[5] Mark Weber, Daniel Karl I. Weidele, Giacomo Domeniconi, Claudio Bellei, Charles E. Leiserson, Jie Chen, Tom Robinson, “Anti-Money Laundering in Bitcoin: Experimenting with Graph,” 31 June 2019. [Online]. Available: https://arxiv.org/pdf/1908.02591.pdf. [Accessed 3 March 2022].

[6] Dinesh Srivasthav P, Lakshmi Padmaja Maddali,Vigneswaran R, “Study of Blockchain Forensics and Analytics tools,” *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS),* 2021.

[7] Bitqquery, “Bitquery,” 18 August 2020. [Online]. Available: https://bitquery.io/blog/best-blockchain-analysis-tools-and-software. [Accessed 12 March 2022].

[8] Originstamp, “Originstamp,” Originstamp, 8 September 2022. [Online]. Available: https://originstamp.com/blog/what-is-blockchain-analytics-and-how-does-it-work/. [Accessed 15 September 2022].

[9] W. Kenton, “Investopedia,” Investopedia, 31 July 2020. [Online]. Available: https://www.investopedia.com/terms/e/exchange.asp. [Accessed 26 February 2022].

[10] R. Sharma, “Investopedia,” Investopedia, 21 September 2022. [Online]. Available: https://www.investopedia.com/decentralized-finance-defi-5113835. [Accessed 24 September 2022].

[11] Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, Tarun Chitra, “Cornell University,” 8 November 2019-2021. [Online]. Available: https://arxiv.org/abs/1911.03380. [Accessed 23 February 2022].

[12] Andrey.Sergeenkov, “The beginner´s Guite to Token Swaps,” 1 June 2021. [Online]. Available: https://coinmarketcap.com/alexandria/article/the-beginners-guide-to-token-swaps. [Accessed 12 March 2022].

[13] Luo, Thomas Chen Hui Lu Teeramet Kunpittaya Alan, “A Review of zk-SNARKs,” Arxiv, 14 February 2022. [Online]. Available: https://arxiv.org/pdf/2202.06877.pdf. [Accessed 28 February 2022].

[14] J. Frankenfield, “Investopedia,” Investopedia, 8 January 2022. [Online]. Available: https://www.investopedia.com/terms/h/hot-wallet.asp. [Accessed 1 March 2022].

[15] Ethereum, “Ethereum,” Ethereum, 14 February 2022. [Online]. Available: https://ethereum.org/en/bridges/. [Accessed 2 March 2022].

[16] R. J. Dolor, “Binance Smart Chain (BSC) Explained | A Beginner’s Guide,” FinBold, 30 May 2022. [Online]. Available: https://finbold.com/guide/binance-smart-chain/#Introduction. [Accessed 26 July 2022].

[17] Bybit, “Tornado Cash: How It’s Stirring Up a Storm in the Crypto World,” Bybit, 4 September 2022. [Online]. Available: https://learn.bybit.com/defi/what-is-tornado-cash/. [Accessed 27 September 2022].

[18] M. Shen, “Crypto Mixer Tornado Cash Says Sanctions Can't Apply To Smart Contracts,” 10 March 2022. [Online]. Available: https://www.bloomberg.com/news/articles/2022-03-10/crypto-obfuscator-tornado-says-sanctions-cant-affect-smart-contracts. [Accessed 14 June 2022].

[19] Johannes Krupp,Christian Rossow, “teether: Gnawing at Ethereum to Automatically,” *27th USENIX Security Symposium,* 2018.

[20] Peilin Zheng , Zibin Zheng , Jiajing Wu, Hong Ning Dai, “XBlock-ETH: Extracting and Exploring,” *IEEE Open Journal of the Computer Society 1 (2020),* pp. 95-106.

[21] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, “An Empirical Analysis of Traceability in the,” 13 April 2017. [Online]. Available: https://arxiv.org/abs/1704.04299. [Accessed 24 June 2022].

[22] BBC News, “Squid Game crypto token collapses in apparent scam,” BBC News, 2 November 2021. [Online]. Available: https://www.bbc.com/news/business-59129466. [Accessed 1 July 2022].

[23] A. Sergeenkov, “What Is PancakeSwap? Here’s How to Start Using It,” CoinDesk, 21 April 2022. [Online]. Available: https://www.coindesk.com/learn/what-is-pancakeswap-heres-how-to-start-

using-it/. [Accessed 20 July 2022].

[24] Donovan, “Tracking the Stolen Assets from the Liquid Exchange Hacking: Laundering Process, Exchanges Involved, Post Tornado Cash?,” Sentinel Protocol Team, 31 August 2021. [Online]. Available: https://medium.com/sentinel-protocol/tracking-the-stolen-assets-from-the-liquid-exchange-hacking-acd94e01c762. [Accessed 25 July 2022].

[25] Haozhe Zhou, Amin Milani Fard , Adetokunbo Makanju, “The State of Ethereum Smart Contracts Security: Vulnerabilities, Countermeasures, and Tool Support,” *Journal of Cybersecurity and Privacy 2.2 (2022),* pp. 358-378.