Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Cryptocurrency Fund Appropriation Techniques: Analysis of Strategies for 'Laundering' and Withdrawing Stolen Digital Assets

Dmitry Mikhaylov
National University of Singapore, Singapore

Received 06 Mar. 2025; Accepted 29 Jun. 2025; Available Online 30 Jun. 2025

Abstract

Given the increased international efforts to prevent illicit financial activity related to cryptocurrencies, the study intends to thoroughly examine the complex field of cryptocurrency laundering. The core of our study project is the complex relationships that exist between cutting-edge technologies and strong security protocols in the cryptocurrency space, a dandruff attack. This paper aims to disentangle the process of bitcoin laundering by exploring the intricate webs of deceit. This is a case study applying observational and experimental methods. We have discovered a pattern of cryptocurrency laundering. The first one saw the primary repository start a cyclical fund movement pattern that involved several new addresses. Equal sums are then systematically transferred over a network of new addresses. The criminal then distributed the stolen money among several new addresses after combining it with an equal quantity of money. It then split and merged, and one saw the resultant sum being transmitted to the BitTorrent blockchain. The cyclical trajectory and engagement with extra money were part of the follow-up return to the Tron blockchain. Observation of the ultimate combination of pilfered money with additional monies sent to the cryptocurrency service "JustLend.org". No research has been done on using a dandruff attack to launder cryptocurrency. Thus, it is essential to acknowledge the offender's activities to raise awareness in general.

I. Introduction

The emergence of cryptocurrencies has significantly transformed the global financial landscape. Providing decentralization, fast transactions, and cryptography safety, such digital money as Bitcoin, Ethereum, and Tron has become not only a source of innovations but also an object of criticism. On the one hand, the opportunity of cryptocurrency is doing the opposite, it democratizes money and eradicates the mediators, but on the other hand, this aspect turned out to be a two-edged sword because of the gaming features. These features, anonymity, decentralization, and boundarylessness of the transactional flow have turned cryptocurrencies into a crime-friendly environment in

Keywords cryptocurrency, dandruff attack, illegality, laundering, stolen digital assets

Production and hosting by NAUSS

Corresponding Author: Dmitry Mikhaylov
Dm@deeptech.engineering

doi: 10.26735/CZJK4881

terms of such activities like fraud, ransomware, and money laundering in particular.

The process of laundering cryptocurrencies is convoluted to disguise the source of cryptocurrencies that were bought or sold illegally, and this process can be performed through relays and mixers, in addition to cross-chain flows. A particularly unexplored method is the dandruff attack, which serves as a deception mechanism through which stolen funds are repeatedly circulated among various wallet addresses, making it extremely difficult to track. The overdeveloped anti-money laundering (AML) measures and blockchain analytics have not been effective because of the constitutional counter-laundering practices. The insufficiently detailed academic research regarding the exact functioning of such techniques in real-life situations restricts the possibility of regulators, analysts, and law enforcement to be flexible and adjust appropriately.

Problem Statement

Although increasing efforts have been applied in regulating and tracking cryptocurrency transactions, the prevailing research and enforcement options are insufficiently prepared to contend with the new forms and techniques of money laundering, like dandruff attacks. The absence of published case studies and forensics interferes with the creation of complete tools for detection and prevention.

Research Objectives

Here, we attempted to fill the information gap by conducting a specialized exploration of the incident of a dandruff assault on the Tron and BitTorrent blockchains. The specific objectives aim to:

1. Research the money laundering schemes applied in the case study chosen, especially the transfer network and pattern.
2. Examine the role played by address clusters, mixers, and blockchain bridges in further obfuscating the origin of stolen funds.
3. Examine the efficiency and admissibility of the existing fund monitoring and blacklisting procedures used in the process of dealing with the case.
4. Determine which technological vulnerabilities and policy blind spots there are that can be used against such attacks.
5. Provide suggestions towards the enhancement of blockchain AML tools and increased transparency in crypto transactions.

Our research should bring value to why the process of cryptocurrency laundering works and be able to help create a more stable and safe digital financial infrastructure.

Research Questions

1. Which laundering techniques were actively used in the example of the dandruff attack on the Tron blockchain and the BitTorrent blockchain?
2. What are the contributions of how to address clusters, repeated fund cycling, and blockchain bridges, trying to create confusion in the pathway of illicit assets?
3. How effectively were there already established fund monitoring and blacklisting mechanisms applied in monitoring or stopping the stolen funds?
4. What are the weaknesses of the blockchain systems and regulatory activities that facilitated the process of laundering?
5. What do the forensic investigations into the dandruff attacks teach us in terms of future developments in the AML frameworks and policy of cryptocurrencies?

Background

Cryptocurrency laundering is an advanced and ever-developing series of processes that focus on hiding the source of criminal-acquired digital funds. Such assets are usually obtained by conducting crimes like ransomware attacks, fraud, and unauthorized access to wallets and exchanges [1]. The essence of these laundering mechanisms is a tactical approach to convert the so-called tainted cryptocurrencies into seemingly clean money so that the perpetrators can incorporate them into the mainstream economy without ever setting off the detection systems. The consequences of such

operations are extensive enough since they make the monetization of cybercrime possible, in addition to damaging the integrity and legitimacy of the wider cryptocurrency economy [1].

Technological versatility and decentralization of the blockchain systems show in the manner in which they were used to engage in cryptocurrency laundering [2]. The most famous ones are mixers and tumblers- services that pool transactions of many users and divide them into randomized denominations, which finally breaks the connection between the sender and recipient of a transaction [3]. This hiding makes tracing on an inherently transparent blockchain extremely difficult. The second one is layering, a process of transfers over a network of addresses, currencies, and exchanges that is complex and multi-staged to obscure the trail of transactions [3].

Other mechanisms that the launderer can use are anonymous wallets, exchanges with peer-to-peer (P2P), and stolen identities. The methods establish the informational blind spots by circumventing the centralized supervision and Know Your Customer (KYC) system [4]. In particular, P2P platforms have been characterized as high-risk settings that allow direct transfers of assets and little regulatory oversight. In the meantime, the elements of identity theft enable criminals to enroll with false identities, which makes it much more challenging to link illegal activity with real-life participants.

Criminal funds have a safe place with the help of offshore accounts offered in a jurisdiction with low enforcement of the law [5]. In the same manner, the token swaps or exchanging one cryptocurrency for another across various networks are frequently deployed to bypass the compliance measures, making the issues of law enforcement and regulatory bodies more difficult to address.

Although blockchain is transparent by nature, these money-laundering techniques take advantage of the lack of real-world identities that wallets provide and the ease of traffic across the networks to build complex money-laundering networks. Although the immutability of blockchain holds the promise of being able to investigate, it also proves to be a problem when a multi-address, multi-chain obfuscation solution is used. Consequently, the financial intelligence and cybersecurity industry still suffers due to a lack of scalability and accuracy in identifying malicious activity.

In its turn, global regulators have advocated increased levels of KYC/AML compliance, especially among centralized exchanges, with an emphasis on non-governmental analytics companies working closer with law enforcement agencies [3]. Nevertheless, the measures that are taken usually fall behind the innovative laundering techniques of these other advanced players, including state-sponsored hacking gangs.

There is an increasing mass of studies aimed at both comprehending as well as modeling laundering operations with the aid of blockchain analytics applications and forensic tracing. However, a significant amount of research has stuck to familiar strategies like mixers, tumblers, and the simple layering, leaving relatively little discussion of the emerging and more clandestine methods of laundering money.

The Novelty and Contribution of the Dandruff Attack Case

The present study fills a large gap in existing literature as it represents the first written assessment of a so-called dandruff attack - a laundering technique involving repetitive movement of funds across high-turnover clusters of addresses, complemented by cross-chain obfuscation and taint dilution by layering transactions. The case is a real-time theft and laundering on the Tron and BitTorrent blockchains, providing a glimpse into the game as a laundering process that eventually removed the tainted status of stolen money and allowed it to be interoperated into legitimate DeFi services.

The dandruff attack on established methods is that it innovatively applies cyclic address loops, tactical blending of funds, and funds laundering through bridges to create both the camouflage of operations and the renewal of transactions. In contrast to, e.g., one-time mixers or low-tech layering, it can emulate realistic transaction workflow at a large scale, which makes automated taint analysis techniques more difficult to recognize.

It is a great contribution to researchers and practitioners. Not only is it an expansion of the taxonomy of laundering methods, but it also points to

the disclosure of technical gaps in the monitoring and policymaking applications of blockchains. Due to the step-by-step analysis of this laundering process combined with the identification of its forensic traceability, the study provides actionable insights into the development of the next-generation AML systems, cross-chain tracking tools, and real-time compliance mechanisms.

Research Aim

This paper targets a systematic exploration and a subsequent report of the mechanisms, structure, and forensic trace of a new method of cryptocurrency laundering that is called the dandruff attack. The research aims to underline how stolen digital assets can be confused and re-entered into circulation through cyclical address clustering, cross-chain asset migration, and taint dilution by carrying out a detailed case study of fund appropriation on the Tron and BitTorrent blockchains. The aim of it all is to establish on the already existing taxonomy of laundering methods, highlight areas of blind detection within the current anti-money laundering (AML) systems, and offer practical advice on the means of improving the blockchain forensic strategies and controlling measures.

II. Literature Review

Cryptocurrency Criminality

In textual composition, one must not solely concern oneself with grammatical mechanics and lexical prowess; rather, one should delve into perplexity and burstiness. The intricate interplay of perplexity fosters profundity and intricacy within the narrative. At the same time, burstiness infuses the prose with a symphony of rhythms and an array of variances. It is this equilibrium between these attributes that begets a truly captivating composition.

Behold the following exposition, bearing a nexus with the landscape of cryptocurrencies. In the year of our data scrutiny, 2021, the crescendo of criminal incidents interconnected with cryptocurrencies reached unprecedented zeniths. A staggering $14 billion illicitly flowed into clandestine accounts throughout this temporal expanse, a surge of significance from the erstwhile sum of $7.8 billion witnessed in the antecedent year 2020 [6]. Yet, let it be known that these numerical reflections provide only a fractional visage of the panorama.

A momentous revelation emerges, wherein the proliferation of cryptocurrencies is undergoing an unparalleled metamorphosis. Across the entire continuum of cryptographic entities under the watchful gaze of [7], the totality of transactional magnitude catapulted to an astonishing $15.8 trillion in the annum of 2021, an astronomical augmentation of 567% when juxtaposed against the metrics of yesteryear.

In this milieu of explosive embracement, the burgeoning legion of cyber malefactors is capitalizing upon cryptocurrencies, which evokes little surprise. Astonishment, however, unfurls its banner when one contemplates the ascension in the volume of unlawful transactions, a meager 79% increment, conspicuously dwarfed by the overarching adoption rate—a discrepancy of nearly an order of magnitude [7].

TraNon-Actional Dynamics in Cryptocurrencies

Indeed, with the dominion of lawful cryptocurrency employment outpacing its illicit counterpart by a substantial margin, the proportion of nefarious exploits within the matrix of cryptocurrency transactional amplitude attains nadirs hitherto unfathomable. In the Chronicles 2021, transactions entwining delinquent accounts constitute a paltry 0.15% of the comprehensive cryptocurrency transactional sphere, notwithstanding the formidable numerical echelon of malevolent transactions cresting unprecedented pinnacles [7].

A modicum of circumspection is advisable, as this numerical embodiment is subject to alteration. Chainalysis, in its unwavering endeavor, continues to unearth addresses woven into the tapestry of unlawfulness, assimilating their transactional chronicles into the annals of history. For instance, antecedent iterations of the Crypto Crime Report bore witness to 0.34% of the cryptocurrency transactional essence in 2020, clasped in the embrace of illicit conduits—a metric since revised to 0.62% [7].

Shifting Landscape of Money Laundering

Cyber culprits who exchange cryptocurrencies commonly share a cardinal aspiration: the

seamless transference of their unlawfully garnered assets to a haven immune to custodial gaze, poised for subsequent alchemical transmutation into conventional currency. This underscores the centrality of money laundering as the cornerstone of a cornucopia of cryptocurrency-tethered transgressions. Should avenues to ingress these assets meet obstruction, the inducement to partake in cryptocurrency-centric misconduct dwindles precipitously[16].

Furthermore, the specter of money laundering within the dominion of cryptocurrencies congeals its manifestations within finite enclaves. Amid the multibillion-dollar cascade of cryptocurrencies from delinquent coffers annually, the bulk meanders into a surprisingly minute coterie of services, many redolent of tailored infrastructures for laundering lucre, given their transactional histories. Through the dislocation of these services, the arm of legal enforcement inflicts a potent stroke against cryptocurrency-infused criminality, imperiling the felonious cohort's capacity to access their digital holdings [17].

The aggregate landscape of cybercriminal activities in cryptocurrency has been laundering an astounding sum exceeding $33 billion in cryptocurrency value since 2017 [6]. This intricate milieu has been predominantly marked by the prevalence of such transactions occurring within centralized exchanges over time. However, a pivotal shift in this trend was discerned in the preceding year. Notably, for the first instance since 2018, the proportion of funds originating from illicit sources that found their way into centralized exchanges dwindled to a mere 47% [7].

Implications of DeFi Adoption

This prompts a thoughtful inquiry: Where did the purveyors of cybercriminal endeavors channel their financial resources? The decentralized finance (DeFi) protocols notably absorbed the deviation, marking a transition of paramount significance. Specifically, in 2021, DeFi protocols emerged as recipients of approximately 17% of the funds emanating from illicit origins [7]. This marked a substantial surge from the mere 2% witnessed in the antecedent year.

The implications of this progression are far-reaching, amounting to an astonishing year-on-year escalation of 1,964% in the aggregate value allocated to DeFi protocols from sources of an illicit nature. The cumulative quantum of this capital influx translated into an impressive $900 million during the year 2021 [7]. Furthermore, the precincts of mining pools, high-risk exchanges, and mixers have also witnessed substantial upswings in the valuation derived from unscrupulous addresses.

Escalating Scams and Theft

As elucidated in prior discussions, the tenor of money laundering activities tends to merge within a select cluster of services. The temporal trajectory of this concentration is elucidated in the ensuing exposition. Although a superficial ascent in the concentration of money laundering activities is discernible due to the curtailed utilization of services in the year 2021, more nuanced scrutiny at the level of deposit addresses serves as a more revealing lens [8]. This is particularly germane given the intricate operational modus operandi of numerous money laundering services, which often function as nested entities, leveraging addresses hosted by more sizable platforms to tap into their liquidity and trading pair potential. Illustratively, over-the-counter (OTC) brokers frequently inhabit the role of nested services, replete with addresses domiciled within major exchanges [8]. A graphical depiction now presents all service deposit addresses that received untoward funds in 2021, categorized following the gamut of illegitimate funds received.

It is instructive to note that while the concentration of money laundering activities endures, its intensity is less pronounced than in the preceding year of 2020. During that temporal juncture, a substantial proportion of 55% of all cryptocurrency translocated from disreputable addresses was siphoned into a mere 270 service deposit addresses [9]. Plausibly, it is conceivable that certain money laundering services relinquished their operational pursuits in the wake of concerted actions against illicit platforms. This compelled cybercriminals to diversify their laundering endeavors across an array of operators. Alternatively, the operational conduct of money laundering services

might have persisted, albeit diversified across a more comprehensive array of deposit addresses.

Noteworthy expansions manifest in two discernible categories: the embezzlement of stolen funds and, to a more modest extent, the perpetration of scams. The expanse of the DeFi domain plays a pivotal role in the trajectory of both these categories [9].

Turning attention to the domain of scams, the fiscal proceeds garnered from such nefarious activities underwent an impressive surge of 82% throughout 2021, culminating in the misappropriation of cryptocurrency assets valued at $7.8 billion [7]. A substantial share amounting to $2.8 billion, which notably approximates the increment observed in the cumulative valuation of 2020, was ascertained to have originated from instances colloquially known as "rug pulls." This nascent chicanery entails formulating ostensibly legitimate cryptocurrency projects, surpassing the mere establishment of wallets to ensnare investments under the veneer of fraudulent prospects. This endeavor culminates in the flight of developers and the commensurate absconding of investor funds. It is imperative to underline that the reported losses attributed to rug pulls exclusively encapsulate the purloined value of investor funds and do not extend to encompass the subsequent diminution in the value of DeFi tokens following the incidence of a rug pull.

In the landscape of blockchain and cryptocurrency, a poignant illustration emerges in the saga of rug pulls during 2021. Notably, an overwhelming 90% of the losses attributed to rug pulls during this period were traceable to a singular fraudulent centralized exchange, Thodex [7]. Eerily, the CEO of this platform vanished into obscurity shortly after user withdrawal capabilities were suspended. A notable observation reveals that the remaining rug pulls documented by [7] in 2021 found their roots in the domain of Decentralized Finance (DeFi) projects. Developers ensnared investors into acquiring tokens linked to DeFi endeavors in these instances. Subsequently, the developers dissipated the invested assets, precipitously causing the tokens' value to plummet.

The prevalence of these rug pulls within the DeFi arena can be attributed to intertwined factors. Firstly, the enthusiasm enveloping this sphere has played a pivotal role. The transaction volume within DeFi experienced an unprecedented surge of 912% during 2021 [7]. The allure of substantial gains, exemplified by tokens such as Shiba Inu, ignited widespread speculation on DeFi tokens. Moreover, individuals well-versed in the requisite technical intricacies can facilely generate new DeFi tokens, ushering them onto exchanges, frequently without comprehensive code audits. A code audit necessitates external scrutiny by a third-party entity or a listing exchange. This process rigorously evaluates the smart contract's code underpinning a novel token or DeFi project. The objective is to ensure the robustness of governance principles and the absence of mechanisms enabling developers to abscond with investors' assets. Many investors could have averted losses by emphasizing DeFi projects that had undergone meticulous code audits. Alternatively, mandating code audits before token listing could have abetted the situation on decentralized exchanges.

Cryptocurrency Theft and Laundering

The specter of cryptocurrency theft loomed ever more prominent, with a staggering $3.2 billion in digital assets pilfered in 2021. This marked an exponential escalation of 516% compared to the preceding year. Intriguingly, $2.2 billion of these ill-gotten gains, constituting 72% of the total, were siphoned from DeFi protocols [7]. This uptick in DeFi-associated thefts substantiates a trend recognized in the previous year's Crypto Crime report.

To contextualize the progression, 2020 witnessed a slightly under $162 million heist from DeFi platforms. This amounted to 31% of the overall crypto theft for the year, signifying a remarkable augmentation of 335% compared to 2019 [7]. By 2021, this figure exhibited an astounding upsurge of 1,330%. The expansion of the DeFi sector was congruent with an escalating issue of misappropriated funds. Naturally, malefactors encountered the intricate chore of laundering the stolen cryptocurrency.

Cryptocurrency laundering entails the intricate art of obfuscating the origin of unlawfully acquired or "tainted" crypto assets, rendering them seemingly legitimate. This endeavor typically seeks to evade detection by law enforcement agencies,

regulatory bodies, and other entities tasked with monitoring financial transactions for anomalies.

Methods of Crypto Laundering

Cryptocurrency laundering involves a multi-step process designed to obscure the origin of funds and construct a convoluted trail that defies easy tracing. Several methodologies are commonly employed to achieve this.

Mixers and Tumblers

Termed coin mixers, bitcoin mixers, or cryptocurrency tumblers facilitate the amalgamation of users' cryptocurrency assets, effectively camouflaging the transaction's source and intent. A complex amalgam of funds emerges by pooling an individual's cryptocurrency with others, rendering it intricate to ascertain their origins. This intricate procedure stands as a means to heighten the anonymity and confidentiality of cryptocurrency transactions [3].

At its core, the coin mixer serves the pivotal function of enhancing the anonymity and confidentiality associated with cryptocurrency transactions. Unlike the conventional banking structure, wherein transactions undergo processing and documentation by financial entities and governmental bodies, cryptocurrencies operate via a decentralized network [4]. While this framework imparts autonomy and freedom, it also exposes transactions to potential tracking, thus risking the exposure of transaction participants.

The coin mixer addresses this concern by intertwining the cryptocurrency holdings of diverse users, generating an indistinguishable pool of resources that evades traceability to the original sender. This complex mingling renders the tracking and identification of transaction participants formidable.

Furthermore, coin mixers introduce an extra layer of defense against cyber intrusions and theft, as they complicate the identification of the sender's address, rendering it an arduous task for malicious actors to ascertain the source.

The precise functioning of a coin mixer can exhibit variations depending on the particular service [4]. Nevertheless, a generic step-by-step outline of the coin mixer process can be delineated:

1. User Initiation: The process commences with a user initiating a transaction, directing cryptocurrency to the coin mixer's address.
2. Mixing Phase: Upon receiving the cryptocurrency, the coin mixer blends it with funds from other users. This typically involves dividing the user's funds into smaller portions and mingling them with other users' holdings.
3. Strategies of Obfuscation: The coin mixer can employ diverse obfuscation strategies, such as transaction delays, routing transactions through distinct wallets, or utilizing varying denominations. These strategies further confound the origin and destination of the funds.
4. Dispersion Phase: After mixing and obfuscation, the combined funds are disbursed to users. Recipients receive cryptocurrency from a collective fund pool without any traceable connection to their original holdings.
5. Transaction Verification: Once the combined funds are disseminated, the transaction attains confirmation on the blockchain.

Coin mixers harness coin mixing and obfuscation techniques to obscure the source and destination of cryptocurrency transactions. These techniques introduce complexities aimed at impeding the traceability of fund movement.

One prevalent strategy entails transaction delay, which entails postponing the processing of transactions for a designated duration [3]. This temporal gap introduces ambiguity into the fund's source, given that the delay creates discontinuities in the transaction history.

Another approach involves routing transactions through distinct wallets. This mechanism leverages intermediary wallets to transfer funds between the sender and recipient. Such multi-wallet routing thwarts easy tracking of fund movement.

Further complexity is introduced through the application of differing denominations. By segmenting funds into disparate denominations and merging them with other users' holdings, the origin of

funds becomes even more intricate to discern. This practice bolsters the layer of anonymity provided.

Layering

The cryptic art of layering involves a choreographed ensemble of transactions traversing diverse accounts, cryptocurrencies, and exchanges. This financial ballet's crux is constructing a labyrinthine money trail, confounding investigators and rendering the origin a mirage [10]. This intricate journey is akin to the meticulous brushstrokes on a canvas, each transaction a nuanced stroke contributing to the enigma. The traversal of funds across wallets, exchanges, and borders emulates breadcrumbs scattered within a forest, an endeavor to bewilder any pursuers.

Each transition between wallets and currencies engenders metamorphosis akin to a chameleon adapting to its environment. This intricate transmutation augments the complexity, inundating the investigative terrain with a surfeit of transactions [10]. Comparable to a well-orchestrated symphony, layering introduces an orchestrated chaos, where timing, rhythm, and path blur the dichotomy between legality and illegality. With layers cascading upon layers, the composite effect engenders a digital problem, fragments dispersed, defying cohesive reconstruction.

Investigators' endeavor to decipher the layered tapestry is akin to reassembling a shattered glass mosaic [1]. Conventional investigative methodologies, efficacious in uncomplicated scenarios, falter in the face of cryptocurrency layering's intricacy. Exploiting the expansiveness of the digital realm, cryptocurrency layering crafts an elusive trail, evading conventional surveillance.

Anonymous Wallets

The emergence of anonymous wallets augments the labyrinthine realm of cryptocurrency laundering, forging hidden alcoves shielding unlawfully accrued gains. These concealed repositories, akin to enigmatic fortresses within the blockchain's labyrinth, exacerbate challenges encountered by authorities in tracing tainted funds. Unlike conventional financial systems necessitating personal identification, anonymous wallets shroud users' identities within a web of intricate code [11].

Malicious actors exploit these wallets to sanitize proceeds from cybercrime, fraud, or ransomware, obfuscating the money's origins behind layers of convoluted code. Law enforcement agencies grapple with this cryptographic conundrum, endeavoring to reconcile newfound financial paradigms with security concerns. The very technologies championed for record preservation, such as blockchain and robust coding, are employed to veil identities [11].

In response, the cryptocurrency sphere and regulatory bodies engage in a delicate equilibrium. Regulatory guidelines stipulate heightened transparency for exchanges and services, accentuating the convergence of privacy and accountability. This dynamic interplay molds the trajectory of digital finance, a narrative oscillating between concealment and oversight [11].

Therefore, anonymous wallets emerge as catalysts in the ongoing narrative of cryptocurrency's evolution, blurring the lines between safeguarding and disclosure. As complexities compound and dynamics evolve, a collective comprehension and flexible adaptability emerge as imperatives in navigating this enigmatic labyrinth. In this perpetual saga, the interplay of concealment and revelation elucidates the intricate tapestry woven by digital currencies.

P2P Exchanges

Peer-to-peer (P2P) exchanges manifest as concealed marketplaces where tainted digital assets undergo a metamorphosis into the veneer of legitimacy. In stark contrast to conventional exchanges, these decentralized platforms facilitate the direct exchange of cryptocurrencies among individuals, circumventing the scrutiny of centralized entities [12]. This nascent trading modality contemplates the ethical and legal ramifications of these platforms.

P2P exchanges constitute a departure from the traditional financial apparatus, allowing participants to engage in direct transactions while eschewing the involvement of established financial intermediaries. Although ostensibly designed to facilitate lawful exchanges, these platforms have

inadvertently provided an enclave for malevolent actors to launder their ill-gotten digital fortunes.

In the domain of cryptocurrency-related criminal activities, P2P exchanges play an influential role [13]. Malicious agents exploit these platforms to locate accomplices to effectuate the conversion of their illicit digital holdings into a semblance of legitimacy. This clandestine exchange parallels subterranean transactions in the physical world, characterized by furtive dealings to evade detection. Analogous to the artistry of a magician's illusion, these exchanges deflect attention from the underlying transactions.

For law enforcement agencies and entities entrusted with the oversight of financial systems, grappling with P2P exchanges presents a formidable challenge. Traditional methods of monitoring established exchanges prove ineffective in this context due to the decentralized nature of P2P platforms [13]. Cryptocurrency transactions within P2P environments frequently transpire via private communications and specialized services, exacerbating the intricacy of tracking the flow of capital.

As technological landscapes evolve, regulatory frameworks and cybersecurity experts strive to achieve an equilibrium between innovation and security. While decentralized exchanges extend enhanced autonomy and privacy to ordinary users, they concurrently furnish opportunities for criminal exploitation [12]. Governments are diligently laboring to implement surveillance mechanisms and control measures to counteract criminal activities while preserving the latitude for legitimate trading activities.

In the narrative recounting the transformative impact of cryptocurrencies on financial paradigms and societal constructs, P2P exchanges serve as a testament to the convoluted nature of emerging domains. Navigating this narrative necessitates balancing fostering innovation and deterring malevolent behaviors. As the narrative unfolds with twists and turns, P2P exchanges are a constant reminder of the imperativeness of vigilance, adaptability, and comprehensive comprehension of the dynamics of cryptocurrency-related malfeasance.

Stolen Identities

In cryptocurrency, the appropriation of stolen identities manifests as a sagacious stratagem. Malfeasants manipulate fabricated or stolen credentials to establish profiles on digital currency platforms. This clandestine maneuver enables surreptitious transactions that elude regulatory scrutiny.

Envision a digital theatrical production wherein characters simulate alternate personas. Analogous to thespians assuming diverse roles, wrongdoers adopt counterfeit identities to participate in the cryptocurrency domain [14]. Feigning authenticity through spurious documentation, they assume the guise of bona fide individuals seeking integration into this realm of virtual currency.

The ramifications of this phenomenon are profound. Culprits leverage purloined identities to infiltrate the domains frequented by law-abiding citizens for legitimate exchanges. These counterfeit accounts serve as conduits for transferring and concealing ill-gotten gains [14]. This deception veils their ulterior motives and obfuscates the scrutiny of authorities tasked with unmasking the authentic operators behind these platforms.

For law enforcement agencies and legislative architects, thwarting this stratagem assumes the guise of a perplexing challenge. The intricate milieu of cryptocurrency presents an onerous conundrum: distinguishing authentic users from malevolent impersonators [14]. As the narrative unfolds and personae evolve, discerning veracity and tracing origins becomes exponentially convoluted.

To counter this predicament, digital currency platforms and regulatory bodies augment their vigilance in identity verification. Stringent protocols are being implemented to corroborate the authenticity of user identities, thereby impeding the endeavors of those seeking to perpetrate falsity. Collaborative endeavors are also being fostered to curtail suspicious account activity.

Offshore Accounts

In the realm of cryptocurrency laundering, the utilization of offshore accounts entails capitalizing on disparities in regulatory frameworks across different nations. Malign actors channel their ill-gotten digital wealth to these remote locales characterized

by lax governance [3]. These distinct regulatory environments provide camouflage for concealing their financial activities and evading detection.

The ramifications of offshore accounts are substantial, transcending geopolitical boundaries and disregarding conventional limits. Cryptocurrencies traverse digital expanses, seeking havens characterized by regulatory frailty. Once ensconced, these digital assets remain veiled from attempts at traceability.

For law enforcement agencies and policy architects, grappling with offshore accounts resembles unraveling a labyrinth with intricacies and twists. Pursuing the trail of digital capital within these pliable regulatory landscapes is akin to navigating a convoluted maze, with each jurisdiction presenting unique challenges [3]. The opacity of cryptocurrencies stems from their decentralized nature, impeding facile attribution to actual individuals or agendas.

Governments and international consortia are collaboratively endeavoring to standardize regulations across jurisdictions. They aim to rectify existing loopholes exploited by malevolent entities leveraging lax regulatory regimes. Yet, achieving global uniformity in financial regulations is akin to navigating a colossal vessel through turbulent waters, demanding patience and meticulous efforts.

Token Swaps

The paradigm of token swaps represents a metamorphic process reminiscent of alchemical transformations. Analogous to chameleons adapting to their surroundings, digital currencies morph and undertake novel roles across disparate networks, orchestrating a convoluted symphony of tokens that elude investigators.

Token swaps entail the transition of one digital currency to another, typically spanning distinct networks [9]. This transcends conventional transactions, akin to the rapid metamorphosis exhibited by magical acts. Criminal entities exploit less-scrutinized digital currencies to veil their illegitimate assets.

The ramifications of token swaps reverberate extensively. The shuffling of funds across digital currencies obfuscates the money trail, culminating in an intricate puzzle for sleuths to solve. Each subsequent swap compounds the intricacy, making identifying the primary source progressively elusive.

Conventional investigative methodologies, predicated upon tracking money within singular networks, prove inadequate in addressing token swaps [9]. The fluid digital ecosystem of cryptocurrencies exacerbates the intricacy, devoid of conventional financial constraints.

In response, experts and regulatory bodies endeavor to devise novel mechanisms for cross-network monitoring. Simultaneously, a collaboration between cryptocurrency stakeholders and regulatory entities emerges as a requisite to thwart these ingenious stratagems.

Token swaps epitomize the duality of innovation and security within the evolving narrative of cryptocurrency's societal impact. As tactics evolve and paradigms shift, countering these strategies necessitates perpetual adaptability, collaboration, and a profound comprehension of these multifaceted actions.

III. Methodology

Research Design

This paper develops a case study design to examine a new method in cryptocurrency laundering dubbed the dandruff attack. More detailed information regarding "dandruff attacks" can be studied in the [15] article via this link. The multi-layered processes of laundering through high turnover addresses clusters, and cross-chain dealings are complex enough to warrant a case study approach. Having concentrated on one real-life laundering event described on Tron and BitTorrent blockchains, the present research produces a profound understanding of laundering mechanics, adversary tactics, and forensic blind spots.

Case Selection and Significance

The trial case concerns the illegal transfer and washing of 50,000 USDT on the Tron blockchain. The first case discovered by Match Systems, the attack includes a novel laundering strategy that involves cyclic money rotations, clustering

corruption, and cross-chain bridging that achieve the final goal of taint dilution of stolen resources.

The specifics of the working process have been chosen in this case:

- Utilization of a massive address cluster that has a billion dollars in total number of transactions.
- Use of repeat cycling and token blending to control asset classification.
- Execution of a cross-chain laundering through the BitTorrent Bridge.
- Conformance to laundering activities involved with advanced actor groups, namely the Lazarus Group.

This scheme of laundering can be recognized as the key to the design of future apps against money laundering (AML) and forensic analytics, as it reveals both technical weaknesses in blockchain infrastructure and regulatory gaps in the existing regulations of compliance.

Case Context and Operational Background

The generation of laundering occurred when one of the victims accidentally sent 50,000 USDT to the address of a scammer on the Tron network. After warnings, Match Systems tagged the wallet in question with the label of having deposited "illicit funds" on large blockchain tracking systems and notified exchanges to attempt to freeze incoming transfers or intercept them. The wallet of the scammer was subsequently thoroughly tracked in order to trace further action.

The laundering plan is similar in structure to the plans deployed in the earlier hacks by Atomic Wallet and AlphaPo, both of which are connected to the North Korean hacker group Lazarus. These events, as well as the case under consideration, have a clear modus operandi which involves the following elements:

1. Employment of services of swaps (SwftSwap, SimpleSwap, SunSwap) without KYC/AML.
2. Inter-chain displacement through interfaces such as the Avalanche bridge or BitTorrent Bridge.
3. Large-scale laundering through the clusters of addresses involves significant volume and speed.

Data Collection and Tools

- The data underlying this study was sourced by analyzing the recordings of public blockchains and third-party analytical tools. The instruments and techniques of it are:
- Blockchain Explorers: TRONSCAN and BitTorrent Explorer were applied in order to access the information on transactions, wallet balances, and the paths of tokens.
- Cluster Analysis: The analysis involved manual and automated tracking of transactions associated with clusters, with the aim of mapping the movement of funds across numerous addresses.
- Taint tracking: heuristics on forensic classification and open AML data were used to verify labels like illicit, clean, and mixed.

Visual Reconstruction: A transaction flow diagram (Fig. 1) has been made to denote the laundry sequence. It shows how the laundering works in the Dandruff Attack, as stolen USDT was hidden with structured steps. Money goes through Cluster A, where roundtripping (20x loops) conceals roots. This is then followed by a long linear transfer chain that combines with another 50K USDT, and after that, a cross-chain jump is done through the BitTorrent Bridge that allows one to anonymize. Having been separated and rejoined, 200K USDT appears on the receiving end, where it enters the Cluster B, a smaller loop intended to mix the money even more. Then the funds are eventually sent to JustLend.org, a DeFi platform, where they are cashed out. Tainted funds are color-coded (red), clustering (orange), cross-chain transitions (blue), and final destination (green). It is an important figure that shows how money laundering schemes are using the limitations of blockchain transparency by combining transactions, cross-chain bridges, and DeFi terminals to launder funds without being dry-cleaned and postponing the identification.

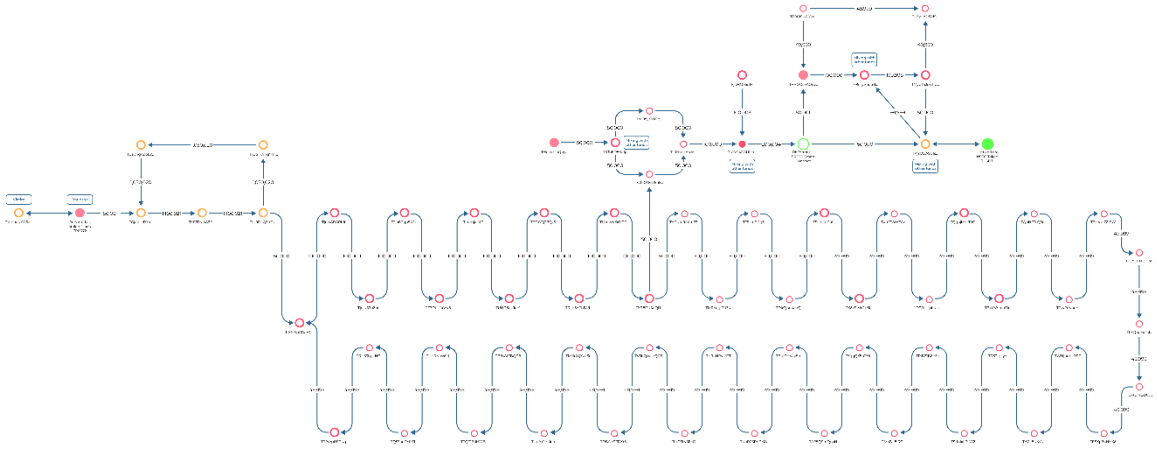

Fig. 1. Funds Laundering Flow through the Tron Network

Analytical Framework

A five-step model was used in breaking down the laundering operation:

1. Construction of Address Cluster

The hacker establishes a transactional arrangement of tens of high-turnover wallet addresses. These additions were achieved by transferring hundreds to thousands of USDT through the address, creating a total transaction volume of more than a few billion USDT. This heavy traffic portrayed the cluster liked a genuine exchange service and therefore the threat was less inclined.

2. First Offshore and Internal Laundering

This address cluster (Fig. 2) was filled with the address verification algorithm to support the 50,000 USDT of dirty money. The financing moved back and forth through the algorithm-based routes through fractional migration. Approximately three-quarters of the total volume of transactions was transferred via SunSwap, which further mixed the assets (Fig. 3). These operations imitated the effect of the conventional mixers and incrementally filtered out prominent taint.

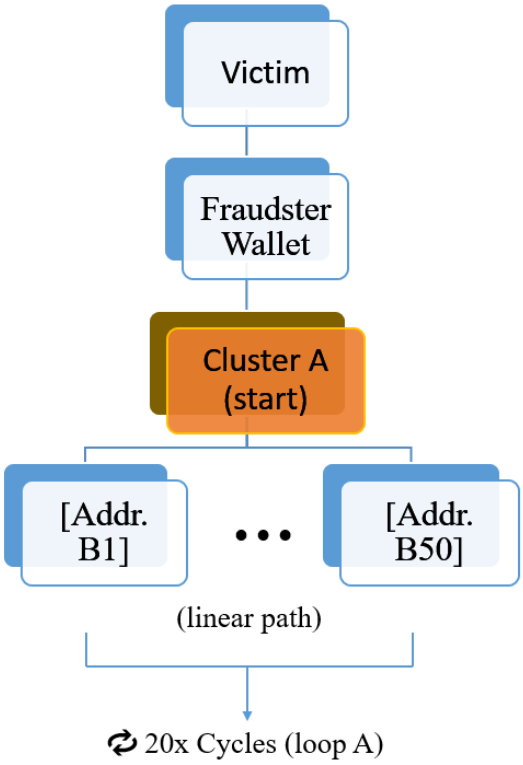

Fig.2. Phase One: Initial Transfer

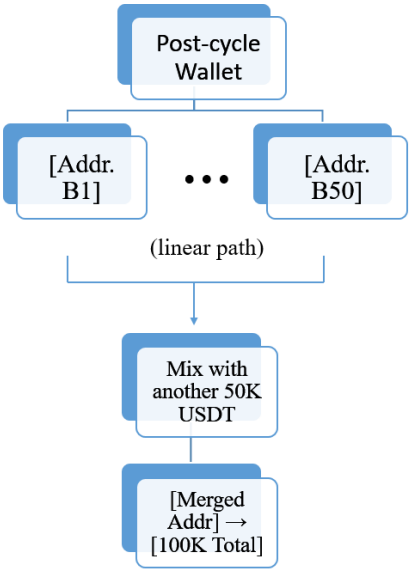

Fig. 3. Phase Two: First Transfer Chain

3. ***Cross-Chain Obfuscation***

Since the first laundering on Tron, the attacker involved a new cross-chain money transfer with the aid of the BitTorrent Chain ERC20 Smart Contract (Fig. 4). After being moved to BitTorrent, the resources were divided and combined with other tokens, after which they were introduced into the Tron blockchain through new accounts. This on-chain hop created a break in on-chain traceability, and it temporarily reset taint flags.

4. Reintegration and Final Taint Dilution

The second mixing cycle took place on Tron, during which the laundered money had been in contact with 150,000 USDT of unrelated funds (Fig. 5). It was directed to JustLend.org, a DeFi site, after several mergers and rotations, so that it can be finally laundered. Now the abused funds are declared clean because it has passed all the conventional screens of taint detection.

5. Validation and Signature Extraction

During every laundering round, taint classification was tracked at major time points to determine the level of obfuscation efficiency. The entire process that the laundering followed was examined in order to get the behavioral signatures out, and how to come up with forensic blind spots, specifically on address clustering and bridge behavior.

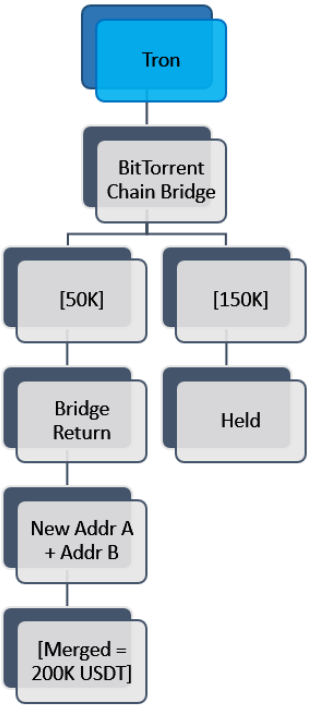

Fig. 4. Phase 3: Cross-Chain Jump

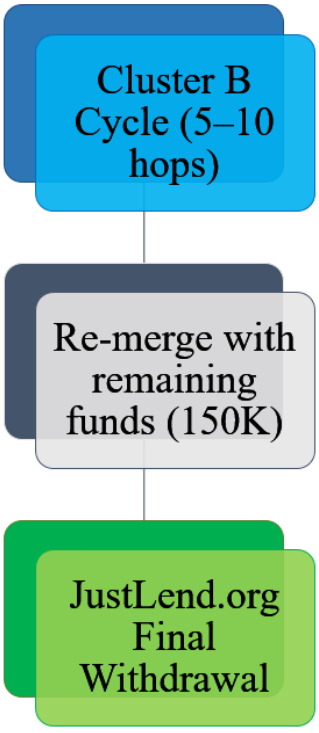

Fig. 5. Phase 4: Final Cycle and Withdrawal

Theoretical and Technological Framework

Transactional obfuscation and financial anonymity networks theories form a basis of the study and refer to previous research on layering [10], token mixing [3], and AML evasion strategies [11]. The technological findings of the research place the dandruff attack in the broader context of the decentralized infrastructure of laundering, which allows illustrating how the DeFi tools, non-compliant swaps, and bridges can be used as a laundering pipeline.

Ethical Considerations

Personally identifiable information has not been accessed and analyzed. All data used on the blockchain was obtained publicly. This study would be prescriptive; it would aim at revealing and reporting on techniques currently applied in criminal laundering to lock down any future surveillance, observation, and policymaking.

IV. Findings and Analysis

In the aftermath of the theft, the fraudster embarked upon a calculated series of actions, ultimately transferring the purloined funds from the designated source. It's imperative to comprehend that these funds bore the unequivocal label of "stolen," a consequence of operational maneuvers executed by Match Systems.

The modus operandi of fund movement followed a structured pattern, meticulously elucidated through visual representation (Fig. 6). Dandruff Attack starts at an early stage, and Fig. 6 illustrates this stage. The wallet of the victim sends 50,001 USDT to the address of the attacker (TP6R72), where the stolen funds were marked. The money then goes into a looping pool where the money of more than 1 million USDT goes through several wallets in a loop pattern. These are mass-sized and similar transactions that are meant to drown forensic tracking with transaction noise and pose as genuine traffic. The loop comes back to the starting point and does not exhibit a distinct way out, which is an indication of laundering action in order to conceal the source and complicate attribution. Let us, in a systematic progression, unravel the sequence:

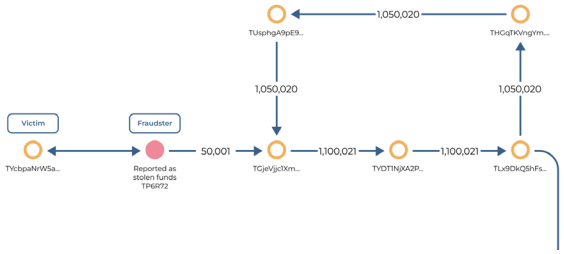

Fig. 6. USDT Fraud and Laundering Case Study

1. Commencing from the primary repository, the perpetrator transmitted a sum of 50,000 USDT to the subsequent address (Fig. 7). This figure reflects the first stage of the laundering operation in which a 50,000 USDT transaction is funneled through a closed loop with five newly generated addresses. The money circulates through more than twenty cycles, forming fictitious transaction volume. This process of making the circular movement pretends to look organic and tries to fool the tainted analysis systems; however, the target it fails at is to reclassify the assets on the way, the funds end up labeled with a 100% stolen designation.

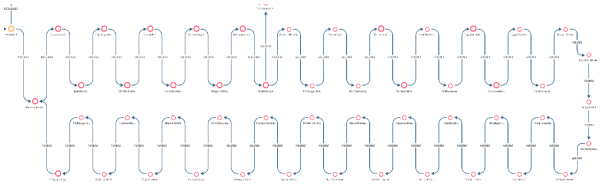

Fig. 7. A recurrent circular journey of the funds through multiple addresses

The course of action effectively precluded the potential cleansing of the stolen assets. Subsequent evaluation of the corpus of funds at the terminal juncture confirmed its unaltered "stolen funds" classification at an unequivocal 100%.

2. Post their egress from the circular paradigm. The malefactor orchestrated the transfer of an equivalent sum of 50,000 USDT into an extensive series of transactions characterized by a network of fifty novel addresses. A subsequent round of

transference ensued, advancing the funds through the continuum (Fig. 8). Fig. 8 indicates the change in cyclic cycling to linear propagation through a network of fifty new addresses. The attacker aims at elongating the sequence of transactions that resemble the work of a regular wallet. Although this may seem elaborate and diffuse, forensic analytics verifies that no amount of dispersion is in effect; the money is well marked as stolen, and thus the inadequacy of the elementary dispersal strategy.

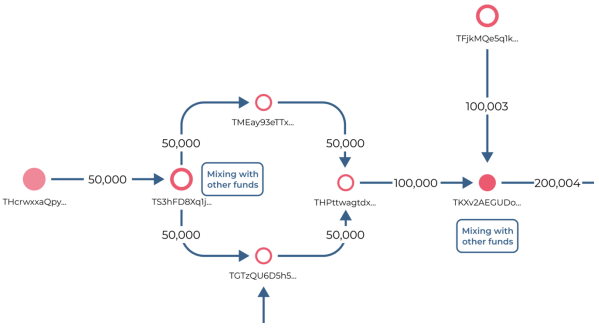

Fig. 8. Mixing and withdrawal attempts

3. Following exiting the prolonged transactional trajectory, the perpetrator intermingled the embezzled sum of 50,000 USDT with an equivalent quantum. This blended amalgamation was dispersed into dual novel addresses and eventually amalgamated anew. Further amalgamation transpired, uniting a total sum of 100,000 USDT, fostering the emergence of a consolidated quantum of 200,000 USDT.
   These maneuvers engendered a partial cleansing of the tainted funds, as they mingled with assets bereft of the "stolen funds" designation. After they departed from this transactional sequence, the resultant composition bore a "stolen funds" classification, albeit at a reduced ratio of 25%.
4. In Fig. 9, the attacker mixes the original 50,000 USDT with an additional 150,000 USDT of untainted funds to rearrange the total 200,000 USDT to the BitTorrent blockchain. The process of the cross-chain transfer and then returning through new accounts assists in resetting the metadata of the transaction. Because of that, the funds are no longer considered stolen by the forensic systems, which once again proves the urgency of cross-chain laundering in erasing the taint.

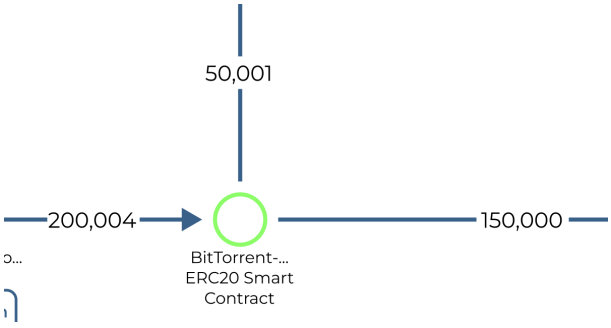

Fig. 9. Post amalgamation actions

5. In Fig. 10, it is evident that on returning to the Tron blockchain, the attacker traffics 50,000 USDT through another loop of five addresses, where there is a fleeting exchange of 100,000 USDT of unmarked funds. This recursion adds even more to the delusion of squeaky clean action. When re-emerged, the 50,000 USDT is taint classified as 0 percent tainted - essentially, it is clean. This step indicates the ability of laundering schemes to take advantage of mixing and transactional density to avoid detection.

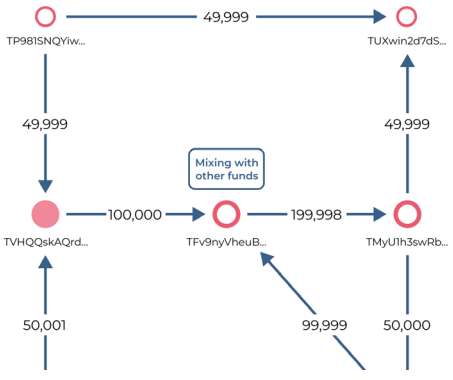

Fig. 10. Results of the Crypto Laundering Process

As a culmination of these actions, the stolen funds retained their untarnished essence, devoid of impurity. Upon departure from this transactional continuum, the funds' composition sustained a "stolen funds" classification of 0%.

6. The final step shows the 50,000 USDT merging with the previously cleaned 150,000 USDT and entering JustLend.org, a DeFi lending platform. This move signifies the successful integration of laundered funds into the decentralized finance ecosystem. The complete erasure of taint by this stage confirms the laundering operation's effectiveness and the need for improved DeFi-based AML protocols (Fig. 11).

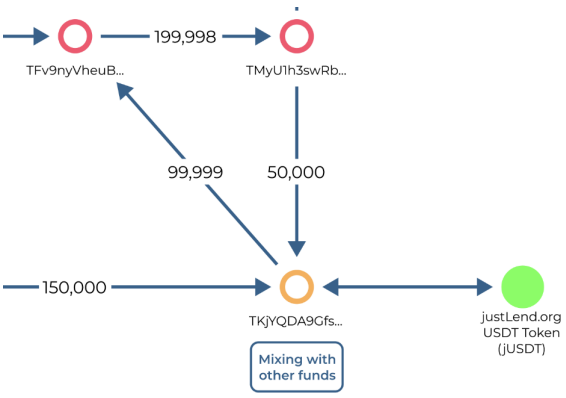

Fig. 11. The Convergence at JustLend.org

V. Conclusion

In the contemporary milieu of cryptographic domains, one must acknowledge the burgeoning scale and the concomitant rise in sophistication exhibited by malevolent actors within the crypto-verse. This palpable escalation underscores the difficult imperative for preemptive measures within the intricate labyrinth of the cryptocurrency ecosystem. As these nefarious elements perpetually refine their methodologies for the obfuscation and repatriation of unlawfully procured digital assets, it is incumbent upon stakeholders to perpetually engage in robust scholarly inquiry and innovation. The security community is poised to discern potential vulnerabilities and construct efficacious counterstrategies by maintaining a proactive stance in deciphering emergent patterns in cybercriminal activities.

Concomitant with the technological purview of laundering illicitly acquired cryptographic assets is the application of intricate clusters featuring an array of numerous addresses, each immersed in a fluidic whirlpool of transactions. An exemplar drawn from practicality entails the meticulous deconstruction of the assorted stratagems deployed by assailants in effectuating the "laundering" and subsequent siphoning of misappropriated resources. It is to be noted, however, that this inventory is merely indicative, for there exist other methodologies that encompass the utilization of cryptocurrency mixers, exchange services predicated upon minimal anti-money laundering (AML) protocols, and sundry other strategies.

Accentuating the complexities posed by malevolent actors in the crypto milieu catalyzes collaborative endeavors among governmental entities, regulatory bodies, and industry constituents. Such a synergetic exchange of perspectives engenders the seamless dissemination of insights, methodologies, and resources requisite for systemic combat against the ever-evolving tapestry of cybercriminal enterprises. Through this united endeavor, the realm of cryptocurrency stands poised to cultivate and actualize regulatory frameworks, technological innovations, and modus operandi that effectively stymie and deter nefarious actors.

Given the burgeoning expanse of challenges posed by crypto assailants, a multifaceted retort is not only justified but imperatively mandated. This response encompasses scholarly research, pedagogical dissemination, and collaborative orchestration. The proactive embrace of these modalities augments the resiliency of the cryptocurrency enclave, poised to counteract the ceaseless metamorphosis of incisive assailants. This collective pursuit forges a secure and robust digital financial landscape in its denouement, catering substantively to diverse stakeholders.

Limitations

Although this study offers a multiprocedural forensic reconstruction of a dandruff attack, there are a number of limitations that limit the generalizability of the study and its findings to a greater extent. First, the analysis is based only on publicly available blockchain data. As much as there are advantages in transparency in blockchain, there are blind areas, especially when the adversaries access the privacy enhancement tools, mixers, or the with broken address hierarchies that cannot be linked deterministically.

Second, by investigating it, the study itself can never look beyond on-chain activity. Off-chain data, including any form of communications, activity on exchange accounts, or social engineering activities, cannot be accessed, but can have a huge impact on the money laundering plan. These vectors of analysis will be veiled without subpoena power or collaboration by centralized services.

Third, systems based on heuristics are used in the classification of taints and fund attribution, and they can result in false positives or an inability to identify new laundering patterns. Labeling of assets as either clean or stolen is driven by the changing detection rules, which fail to capture the more nuanced combination policies or synthetic chains of transactions.

Lastly, the analysis is a focused case-specific approach; although it is highly methodologically rigorous, it might not be sufficient to capture the entire spread of laundering architectures being applied throughout the crypto ecosystem. The actors are free to employ variations of this attack model or even other completely unrelated methods that do not get detected within the existing analytical paradigm.

The study should thus take into account the possibility of integrating off-chain intelligence and extending forensic to the multi-chain interoperability, and providing probabilistic taint models with the ability to identify laundering efforts even in a situation where attribution is non-confident.

Conflict of Interest

Author declares that they have no conflict of interest.

Funding

This article did not receive any specific grants from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] M. W. Calafos, and G. Dimitoglou, “Cyber laundering: Money laundering from fiat money to cryptocurrency,” in *Principles and Practice* of Blockchains, K. Daimi, I. Dionysiou, and N. El Madhoun, Eds. Cham, Switzerland: Springer, 2022, pp. 271–300. doi: 10.1007/978-3-031-10507-4_12

[2] G. Hou, “Cryptocurrency money laundering and exit scams: Cases, regulatory responses and issues,” in *Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies*, S. Corbet, Ed. Berlin/Boston: De Gruyter, 2022, pp. 83–96. doi: 10.1515/9783110718485-007

[3] M. Fröhlich, F. Waltenberger, L. Trotter, F. Alt, and A. Schmidt, “Blockchain and cryptocurrency in human–computer interaction: a systematic literature review and research agenda,” in *Proc. ACM Designing Interactive Systems Conf.* (DIS ’22), 2022, pp. 155-177.

[4] C. Wronka, “Money laundering through cryptocurrencies—analysis of the phenomenon and appropriate prevention measures,” *Journal of Money Laundering Control*, vol. 25, no. 1, pp. 79-94, 2022.

[5] F. Zhou, Y. Chen, C. Zhu, L. Jiang, X. Liao, Z. Zhong, and Y. Zhao, “Visual analysis of money laundering in cryptocurrency exchange,” *IEEE Trans. Computational Social Systems*, 2023.

[6] M. O’Rourke, “Cryptocurrency crime cost a record $14 billion in 2021,” *Risk Management*, vol. 69, no. 1, p. 30, 2022.

[7] Chainalysis, *2022 Crypto Crime Report*. Chainalysis, 2022. [Online]. Available: https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf

[8] S. Pandey, “A study on cryptocurrency with recent development,” *Jus Corpus Law J.*, vol. 2, pp. 366-371, 2021.

[9] D. Lin, J. Wu, Q. Fu, Y. Yu, K. Lin, Z. Zheng, and S. Yang, “Towards understanding crypto money laundering in Web3 through the lenses of Ethereum heists,” *arXiv* preprint arXiv:2305.14748, 2023.

[10] I. Alarab, S. Prakoonwit, and M. I. Nacer, “Competence of graph convolutional networks for anti-money-laundering in Bitcoin blockchain,” in *Proc. 5th Int. Conf. Machine Learning Technologies*, 2020, pp. 23-27.

[11] D. Dupuis and K. Gleason, "Money laundering with cryptocurrency: open doors and the regulatory debate," *Journal of Financial Crime*, vol. 28, no. 1, pp. 60-74, 2020.

[12] A. D. Comolli and M. R. Korver, "Surfing the first wave of cryptocurrency money laundering," *Dept. of Justice J. Federal Law & Practice*, vol. 69, pp. 183-202, 2021.

[13] K. Oosthoek and C. Doerr, "Cyber-security threats to Bitcoin exchanges: adversary exploitation and laundering techniques," *IEEE Trans. Network and Service Management*, vol. 18, no. 2, pp. 1616-1628, 2020.

[14] E. Fulton, "Turning cash to cryptocurrency," in *Cyber Laundering: International Policies and Practices*, 2023, pp. 3-25.

[15] D. Mikhaylov, A. Kutin, J., Anderson, and M. Faleev, "Analysis of the 'Dandruff attack' on the Tron Network: risks, damage assessment, and solutions," *Journal of Information Security and Cybercrimes Research*, vol. 6, no. 1, pp. 1–11, 2023.

[16] D. B. Desmond, D. Lacey, and P. Salmon, "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review," *Journal of Money Laundering Control*, vol. 22, no. 3, pp. 480–497, 2019.

[17] E. Ilbiz and C. Kaunert, "Sharing economy for tackling crypto-laundering: The Europol associated 'Global Conference on Criminal Finances and Cryptocurrencies'," *Sustainability*, vol. 14, no. 11, Art. no. 6618, 2022.