Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario
Dipartimento Di Matematica

Corso di Laurea in Diritto e Tecnologia
Anno Accademico 2022/2023

Titolo tesi:

Rilevamento delle anomalie nella Finanza Decentralizzata: opportunità e minacce dei prestiti istantanei

Relatore:
Ph.D, Alessandro Brighente

Studente:
Edoardo Bedei

Indice

Abstract

La finanza decentralizzata rappresenta un nuovo paradigma nel settore finanziario. Essa si basa su tecnologia blockchain, smart contracts e applicazioni decentralizzate, promettendo un accesso aperto, inclusivo e senza intermediazione a servizi finanziari. La rapida espansione di questa nuova frontiera tecnologica, in ogni caso, porta con sé alcune criticità, in particolare in termini di sicurezza e integrità dei protocolli DeFi.

Il presente elaborato propone un approfondimento del modello di finanza decentralizzata, concentrandosi su vulnerabilità, attacchi e strategie preventive nell'ambito dei protocolli DeFi: ciò fa focalizzandosi su uno strumento finanziario di ultima generazione, il Flash loan. Attraverso l'analisi di casi studio e l'indagine di diversi attacchi, inoltre, si mira a delineare soluzioni proattive per garantire efficacia ed efficienza del nuovo paradigma finanziario e dello strumento finanziario analizzato.

Introduzione

La finanza decentralizzata – DeFi – ha portato una rivoluzione senza precedenti per l'ambiente finanziario, ridisegnando le modalità di accesso, scambio e partecipazione a questo tipo di servizio. Proprio tramite la struttura blockchain e l'utilizzo degli smart contracts, la DeFi promette l'eliminazione dell'intermediazione, offrendo a tutti i partecipanti opportunità di accesso in qualsiasi momento nonché la possibilità di sfruttare strumenti alternativi.

Se, da un lato, questo nuovo paradigma ha attirato l'attenzione di numerosi investitori, sviluppatori e utenti di vario genere, dall'altro, le sue fondamenta non sono impermeabili a sfide e vulnerabilità di certa portata. L'innovazione, invero, velocizza l'adozione dei modelli de qua, ma spesso porta con sé significativi rischi. Ecco che l'elaborato si propone di definire le dinamiche, le sfide e le soluzioni in punto di sicurezza dell'ecosistema decentralizzato, focalizzandosi sulle tipologie di attacchi possibili e sulle strategie preventive all'interno del protocollo DeFi. Attraverso l'analisi della casistica, in particolare delle modalità con cui gli attacchi sfruttano le falle in tale sistema, s'intende delineare le metodologie e gli strumenti atti a disincentivare il rischio e rafforzare il sistema.

L'elaborato si articola in quattro capitoli. Nel primo, si delinea il concetto di Finanza Decentralizzata, focalizzandosi sui principi fondamentali, sui vantaggi e sulle sfide poste da questo nuovo paradigma; il secondo capitolo analizza un nuovo strumento finanziario, il Flash loan – in italiano "Prestito Istantaneo" – sottolineandone il potenziale, attraverso il paragone con l'apertura di credito in conto corrente, nonché i rischi derivanti da un uso illegittimo. Il terzo capitolo propone modelli di rilevamento e difesa, delineando così soluzioni preventive e strategie per prevenire e contrastare attacchi futuri. Infine, il quarto e ultimo capitolo, è dedicato all'analisi di attacchi informatici avvenuti tramite l'utilizzo dei Flash loans, enfatizzando il rischio per le piattaforme che essi comportano; nonché allo sviluppo di rimedi e di soluzioni nel contesto della sicurezza dei protocolli di Finanza Decentralizzata.

Stato dell'arte

1. La Finanza Decentralizzata

Il Termine *Decentralized Finance* - in italiano "Finanza Decentralizzata" – definisce quell'ecosistema formato da tutte quelle nuove applicazioni finanziarie implementate su blockchain, accessibili senza autorizzazione[11]. Per applicazioni DeFi si intende l'insieme di *smart contract* - cc.dd contratti intelligenti - rivolti ai consumatori che, all'interno di tale ambiente trasparente e deterministico, hanno la possibilità di porre in essere logiche aziendali le quali sono a loro volta predefinite[12]. La tecnologia blockchain utilizzata alla base della struttura Defi rappresenta il nucleo centrale, la quale memorizza le diverse transazioni in modo sicuro e fornisce un consenso teorico del gioco attraverso l'emissione di un asset nativo.[13]

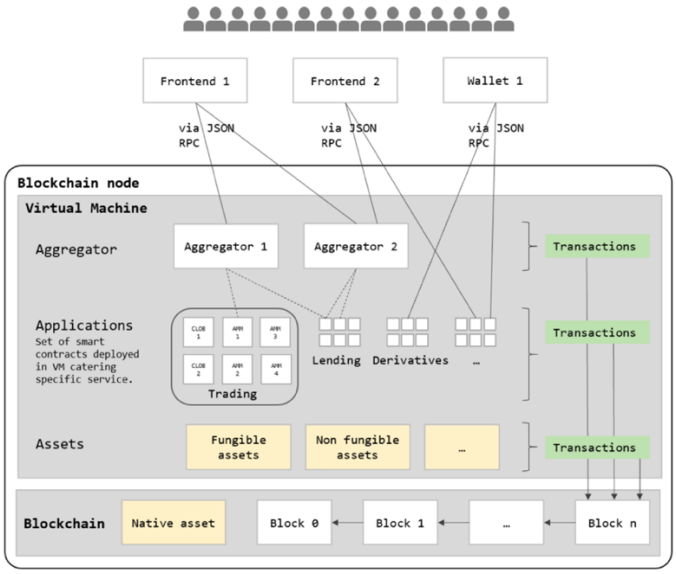

Figura 1: Applicazioni DeFi su blockchain senza permessi [14]

Dato l'ethos open source agli stessi sviluppatori è richiesta la massima trasparenza per la creazione di applicazioni decentralizzate, in modo tale che gli utenti abbiano la possibilità di prendere contezza e di partecipare ai processi decisionali. A tal fine, vengono emessi i cc.dd *token di governance*, ovvero unità detenute da utenti ai quali viene attribuito potere di voto in schemi di voto a maggioranza[15]. Scambiati su mercati secondari, i *tokens*, dando la possibilità di formare capitale, contribuendo allo sviluppo per realizzare applicazioni decentralizzate sempre più scalabili. Tramite la distribuzione di tali asset digitali, i programmatori intendono distribuire ricchezza ai membri della comunità appartenente

---

[11] JOHANNES RUDE JENSEN, VICTOR VON WACHTER AND OMRI ROSS, *An introduction to decentralized finance (DeFi),* pp. 46-47.
[12] I*bid.*
[13] Blockchain technology is the core infrastructure layer (see Figure 1) storing transactions securely and providing game-theoretic consensus through the issuance of a native asset.
[14] JOHANNES RUDE JENSEN, VICTOR VON WACHTER AND OMRI ROSS, *An introduction to decentralized finance (DeFi),* p. 48
[15] Ivi, p. 48

alla blockchain, mantenendo allo stesso tempo un capitale adeguato alla crescita futura dell'architettura stessa. In aggiunta, diversamente a ciò che accade per i sistemi tradizionali utilizzati come per esempio le applicazioni bancarie, gli utenti hanno la possibilità di interagire all'interno del sistema senza l'ausilio di intermediari. [16]

2. I Flash loans

Attraverso l'uso di *smart contracts* - in italiano "contratti intelligenti" - si è aperta la possibilità di creare, nei sistemi *DeFi*, veri e propri strumenti finanziari alternativi. Tra questi, utilizzati nell'ecosistema decentralizzato, vi sono i cc.dd. *Flash loan*s - in italiano "prestiti istantanei" – una nuova tipologia di prestiti che vengono erogati rapidamente e si differenziano da quelli tradizionali propri del sistema CeFi. Questi prestiti, infatti, non necessitano di essere garantiti da collaterali. Inoltre, tali prestiti non comportano sempre degli interessi per la durata, ma solo una commissione di utilizzo a carico dell'utente. Un aspetto interessante dei cc.dd. *flash loans* è che tramite tali strumenti possono essere prestate quantità ingenti di denaro alla sola condizione che queste ultime siano restituite nel corso dell'intera durata della transazione pena la revertazione – dall'inglese *to revert* - dell'intera transazione ossia il ritorno degli asset concessi.[17]

Le principali piattaforme abilitate all'erogazione dei "prestiti istantanei" sono come *Aave*, DydX, UniswapV2.

Aave è stata la prima piattaforma ad aver consentito l'utilizzo dello strumento finanziario tramite una funzione nativa chiamata Flash Loan, con una commissione di utilizzo dello 0,25 % per il prestito erogato. Ai fini dell'erogazione del prestito – cd. *flash loan* - gli utenti devono costruire uno *smart contract* dotato di una funzione di esecuzione e una funzione di ingresso. Con riferimento alla funzione di esecuzione si può dire che essa ingloba gli asset che gli utenti prendono in prestito, come per esempio il trading nelle borse; nella seconda prima gli *stakeholders* preparano la funzione Flash Loan, poi proseguono, di conseguenza, con il contratto executeOperation - contratto ufficiale di Aave - ed infine procedono alla restituzione degli asset erogati dalla piattaforma.

Altra importante piattaforma DeFi è *DydX*, offerente servizi su cryptoasset quali, ad esempio, ETH, USDC. Tale blockchain, a differenza della precedente, non possiede funzioni native, bensì, tramite il contratto SoloMargin, fornisce una funzione che da sola riesce a raggruppare diverse operazioni in un'unica transazione; e – aspetto senz'altro degno di considerazione - non comporta alcun tipo di commissione di utilizzo.

Il *marketcap* di *UniswapV2*, uno dei protocolli DEX più conosciuti, rappresenta una parte rilevante dell'intera liquidità nell'ecosistema analizzato, circa l'11% (3,2 miliardi di USD). Al contrario delle piatteforme precedentemente prese in considerazione, quest'ultima si limita ad implementare, con una commissione dello 0,3 % per l'utilizzo, lo strumento finanziario. Per l'impiego del cd. *Flash loan* gli utenti devono, in primo luogo, definire il codice per l'operazione progettato nella funzione I*UniswapV2Callee*, la

[16] Ivi, pp. 47-48
[17] DABAO WANG, SIWEI WU, ZILING LIN, LEI WU, XINGLIANG YUAN, YAJIN ZHOU, HAOYU WANG, AND KUI REN, *Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem*, p.3.

quale deve contenere al suo interno un'azione di rimborso per il completamento e l'erogazione del prestito[18].

3. L'Anomaly Detection

Il concetto di anomalia viene sviluppato in diversi ambiti. Esistono diverse definizioni del concetto *de qua* in funzione del campo di applicazione e della struttura dati presi, di volta in volta, in considerazione. Tra le differenti esplicazioni del concetto di anomalia proposte, quella più conosciuta è attribuibile a Stephen Hawkins: "*An outlier is an observation which deviates so much from the other observations as to arouse suspicions that it was generated by a different mechanism*"[19].

Un'anomalia può essere originata da una serie di variabili, quali l'errore umano, il guasto strumentale, le deviazioni naturali nella popolazione, le attività fraudolente e i connessi sistemi di rilevamento di queste ultime.

Le tipologie di anomalie si possono suddividere in tre diverse categorie: anomalie puntuali, anomalie contestuali ed anomalie collettive. Definire con esattezza a quale categoria appartiene l'anomalia è di estrema importanza per poter attuare la tecnica di rilevamento più adeguata.

Le anomalie puntuali si caratterizzano quali scostamenti rilevanti di dati. Prendendo in considerazione, a titolo esemplificativo, le carte di credito: una potenziale anomalia potrebbe derivare da un'alterazione dell'importo di acquisto di un determinato bene ravvisabile dal conto corrente.

Le anomalie contestuali – come si evince dalla denominazione - sono istanze di dati anomale in contesti specifici. Vengono utilizzati due attributi per definirle: contestuali e comportamentali. Le prime – istanze contestuali - qualificano quello che è il contesto dei dati; le seconde – comportamentali - denotano quelle che sono le caratteristiche non contestuali.

La terza tipologia - anomalie collettive – infine, racchiude quelle che possono essere definite come una raccolta di dati anomali rispetto all'intero dataset. Determinati eventi, invero, presi singolarmente, potrebbero non essere anomali, ma la loro manifestazione come insieme può essere difforme[20].

---

[18] DABAO WANG, SIWEI WU, ZILING LIN, LEI WU, XINGLIANG YUAN, YAJIN ZHOU, HAOYU WANG, AND KUI RE, *Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem,* pp. 25-26.

[19] WALEED HILAL, S. ANDREW GADSDEN, JOHN YAWNEY, *Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances,* p.3

[20] *Ivi*, p.4

CAPITOLO I
La Finanza Decentralizzata

L'intento del presente capitolo è quello di delineare il sistema della finanza decentralizzata e i suoi principi chiave, sottolineando l'importanza di tale innovazione, tramite un parallelismo tra i sistemi *CeFi* (finanza centralizzata) e *DeFi* (finanza decentralizzata).

1.1 La finanza decentralizzata: definizione e caratteristiche

La Finanza Decentralizzata può essere definita come nuovo paradigma, il quale modifica il concetto base per cui i servizi finanziari non dovrebbero più dipendere esclusivamente da intermediari centralizzati, quali banche, broker, borse valori, bensì essere erogati da utenti per utenti, tramite un'implementazione di rete *peer-to-peer*, così da far comunicare finanziariamente i membri della comunità, tramite prestiti, speculazione su asset e diversificazione[21].

Tale spinta innovativa si deve a due fattori: da un lato, all'automazione - già presente da decenni: basti pensare ad addebiti diretti o ai controlli – dall'altro, alla nuova tecnologia blockchain, per tale intendendosi "un registro di contabilità condiviso e immutabile che facilità il processo di registrazione delle transazioni e la tracciabilità degli asset in una rete commerciale"[22].

La portata innovativa di un sistema di Finanza Decentralizzata può essere rappresentata mediante la comparazione con un sistema finanziario tradizionale ove si ha una relazione tra consumatore/utente e banca, broker e borsa valori, per l'acquisto e la vendita futura del titolo, da cui deriva un addebito per la prestazione del servizio, a carico del consumatore, e potenziali errori durante il processo sopracitato. Specularmente, nella Finanza Decentralizzata tale processo è differente: un utente, tramite il proprio smartphone e con una connessione internet, ha la possibilità di accedere direttamente a una "borsa decentralizzata" – cc.dd. *DeX* - dove può formulare domanda di acquisto per un determinato bene digitale o un c.d. *token*. Quest'ultimo, una volta acquistato, in ragione del fatto che non è presente un soggetto intermediario, viene trasferito direttamente nel portfolio dell'utente. Non solo: tale transazione presenta caratteristiche autentiche. Tra queste spicca senz'altro l'anonimato[23].

Inquadrato rapsodicamente il sistema di Finanza Decentralizzata, si può procedere, in prima battuta, a delineare quelle che sono le caratteristiche che distinguono un sistema tradizionale o centralizzato dal sistema *de qua*: decentralizzazione, non fiducia, anonimato, accessibilità, trasparenza, assenza di autorizzazione e, non meno importante, assenza di regolamentazione.

Innanzitutto, il sistema è decentralizzato in quanto esso si basa sulla tecnologia blockchain, la quale permette di replicare l'informazione sui diversi e numerosi nodi della struttura. Di poi si tratta di sistemi *trustless* poiché, basandosi su blockchain, si parte dal presupposto che in tali sistemi i livelli di sicurezza siano estremamente elevati, e, dunque,

---

[21] PATRICK SCHUEFFEL, *DeFi: Decentralized Finance - An Introduction and Overview*, p. 1.
[22] https://www.ibm.com/it-it
[23] PATRICK SCHUEFFEL, *DeFi: Decentralized Finance - An Introduction and Overview*, p.2.

che non sia necessario un organo di vigilanza per assicurare fiducia all'interno della rete. Per antonomasia, inoltre, le tecnologie *blockchain* sono anonime: la conseguenza è che qualunque utente può partecipare alla rete senza doversi identificare. Altra caratteristica delineata è l'accessibilità: il sistema di Finanza Decentralizzato è utilizzabile da chiunque voglia accedere ai servizi finanziari erogati dalla piattaforma. Ancora: caratteristica fondamentale dei sistemi *de qua* è la trasparenza che denota la componente software sottostante la struttura analizzata. Essendo la Finanza Decentralizzata in grande misura open-source, inoltre, l'accesso e l'utilizzo non sono subordinati ad alcun tipo di autorizzazione: ciò significa che all'utente, una volta effettuato l'accesso alla struttura dati, non deve essere fornita autorizzazione per lo sviluppo di applicativi DeFi, da un soggetto sovrano o da un soggetto intermediario. In ultima istanza, la Finanza Decentralizzata non è regolamentata. Tale caratteristica si giustifica alla luce degli attributi sopra citati: se un sistema è decentralizzato e anonimo nessuna autorità di regolamentazione ha il potere di interferire sul suo funzionamento[24]. In sistemi come quelli suddetti, il controllo pertanto è demandato all'utente il quale diviene custode dei suoi beni/asset, poiché nessun'altro ha la possibilità di censurare, spostare o distruggere ciò che detiene l'utente senza l'autorizzazione di quest'ultimo.

Characteristic	Traditional Financial Services	DeFi - Decentralized Finance
Degree of automation	Low	High
Network Structure	Centralised	Decentralized
Self-custodial	No	Yes
Trustless	No	Yes
Technology importance	Low	High
Intermediary importance	High	Low
Costs of service	High	Low
Product Focus	High	Low
Single Point of failure	Yes	No
Counterparty risk	High	Low
Anonymous	No	Yes
Inclusive	No	Yes
Transparent	No	Yes
Open Source	No	Yes
Permissionless	No	Yes
Flexibility	Low	High
Security	Low	High
Regulated	Yes	No

Figura 2: un confronto relativo delle caratteristiche: DeFi vs. Finanza tradizionale[25]

Al fine di facilitare l'individuazione dei punti di forza del sistema decentralizzato, soccorre la tabella soprastante, la quale sintetizza e metti in relazione le caratteristiche appena elencate con i sistemi di finanza tradizionale.

1.2 Gli Asset della Finanza Decentralizzata

Definito il sistema di Finanza Decentralizzata la domanda da porsi concerne i tipi di *assets* all'interno della struttura appena analizzata.

[24] *Ivi,* p.3

[25] PATRICK SCHUEFFEL, *DeFi: Decentralized Finance - An Introduction and Overview*, p. 4

Per essere scambiato un *asset*, sia esso un titolo di una nuova impresa, petrolio grezzo, servizi di consulenza e vendita di diamanti, vendita di opere d'arte, fino al valore legale della moneta; deve essere, anzitutto, trasformato in *token digitale*. Questo processo viene denominato *Tokenizzazione dell'asset* o Dematerializzazione. Ogni tipo di asset può essere tokenizzato e, in prima battuta, proposto agli investitori tramite la c.d Offerta iniziale di moneta (ICO)[26]. Un *token* - o *cryptoasset* – altro non è che "un insieme di informazioni digitali registrate su una blockchain in grado conferire un diritto a un determinato soggetto"[27]; quindi, esso è a tutti gli effetti "un documento, ossia la rappresentazione di una posizione giuridica su un bene o di una pretesa verso un determinato soggetto"[28].

1.3 Parallelismo tra Finanza Decentralizzata e Finanza Centralizzata

Come detto precedentemente, l'avvento della Finanza Decentralizzata ha portato a un mutamento nel paradigma di finanza, per tali intendendosi "*the process that involves the creation, management, and investment of money*"[29], che nella finanza centralizzata coinvolge tre componenti: l'istituzione, lo strumento utilizzato e il mercato[30].

In aggiunta alle caratteristiche già delineate, meritano di essere considerati ulteriori aspetti che contribuiscono a differenziare questo nuovo paradigma dalla finanza tradizionale.

Prima fra tutti l'atomicità. Una transazione blockchain supporta azioni sequenziali, le quali combinano una moltitudine di operazioni finanziare. Questa combinazione è atomica: il che significa che o tutte le azioni vengono eseguite, oppure falliscono insieme. Tale caratteristica non si ravvisa nei sistemi centralizzati, salvi eventuali accordi legali futuri. Ancora, un altro aspetto è la malleabilità dell'ordine di esecuzioni. Nella rete *P2P*, gli utenti condividono pubblicamente le transazioni che saranno eseguite. A causa dell'assenza di un'entità centrale che ordini l'esecuzione, i peer possono eseguire test di offerta sulle commissioni delle transazioni eseguite per indirizzare l'esecuzione delle stesse. Nelle CeFi, invece, gli organismi impongono regole rigide ai servizi e alle istituzioni finanziarie, al fine di definire l'ordine delle transazioni. Non meno importante è l'analisi dei costi di transazione, indispensabili all'interno dei sistemi Decentralizzati per evitare e prevenire lo "spam". Al contrario, il vantaggio delle CeFi è proprio quello di poter proporre soluzioni senza costi di transazione, affidandosi a verifiche KYC/AML dei loro utenti.

Altra rilevante discrasia rispetto ai sistemi centralizzati sono gli orari di mercato senza interruzione. Un esempio lampante sono le Borse di New York e Nasdaq -principali borse Statunitensi – aperte dal lunedì al venerdì, nella fascia oraria tra le 9.30 e le 16.00. Nei DEX, trattandosi di sistemi basati su blockchain, non vi è interruzione: si tratta di mercati sempre aperti.

---

[26] *Ivi*, p.4
[27] MARCO CIAN, CLAUDIA SANDEI, *Diritto del Fintech, p. 280*
[28] *Ibid.*
[29] KAIHUA QIN, LIYI ZHOU, YAROSLAV AFONIN, LUDOVICO LAZZARETTI, ARTHUR GERVAIS, *CeFi vs. DeFi -Comparing Centralized to Decentralized Finance*, https://www.cornell.edu/admissions/, p.2
[30] *Ibid*.

Inoltre, sono note diverse interruzioni avvenute nella CeFi derivanti da una moltitudine di richieste a fini speculativi: si pensi allo *short squeeze* di Gamestop; per non parlare delle società intermediarie limitanti l'acquisto e la vendita di terminati prodotti finanziari a causa di liquidità, solvibilità nonché dei limiti legali[31].

1.3.1. Il sistema dei controlli

Per quanto attiene agli aspetti legali dei due sistemi, si possono evidenziare differenze significative nell'*onboarding*, nonché nella conformità continuativa e nella fungibilità degli asset.

Per quanto attiene ai sistemi tradizionali, l'utente si trova assoggettato ad una procedura di verifica rigorosa e conforme alla *KYC*, implicante la verifica del documento di identità, - o in alternativa del passaporto o della patente - e l'esigenza di comprovare il proprio indirizzo di residenza. Il tempo necessario a tale verifica può variare, da poche ore a molte settimane, in base al background finanziario dell'utente verificato. In DeFi tale procedura si caratterizza per una maggiore libertà iniziale. Non si può tacere però come anche le applicazioni decentralizzate richiedano inizialmente una verifica KYC ai fini della registrazione dell'utente: si ravvisa qui un punto di interconnessione tra i due settori.

Connaturate ai sistemi centralizzati sono anche le verifiche *AML* (*Anti Money Laudering*), funzionali a definire l'origine, la destinazione e lo scopo degli asset compravenduti da parte delle istituzioni finanziare, allo scopo di evitare e combattere il riciclaggio di denaro. In molte strutture giuridiche, alla base dei mercati centralizzati, si trova incardinato un soggetto incaricato della verifica e segnalazioni di tali anomalie.

Per la particolare struttura dei mercati decentralizzati le istituzioni tradizionali intensificano i controlli al fine di prevenire e disincentivare il riciclaggio di denaro in tali ecosistemi. Rischio – quello che in tali sistemi si ricicli denaro – che è in parte scongiurato dalle stesse caratteristiche dei sistemi decentralizzati: in ragione della trasparenza, che connota tali sistemi, il tracciamento e il riconoscimento delle transazioni all'interno della rete è molto più semplice. Proprio per tale motivo ci si aspetta che le istituzioni centralizzate accettino gli asset del mercato decentralizzato. Asset e transazioni all'interno dell'ecosistema DeFi sono, per l'appunto, tipicamente trasparenti e tracciabili. Così che risulta agile intraprendere processi verifica e poter semplificare e dunque fornire alle autorità CeFi delle informazioni estremamente utili.

Nondimeno residua la possibilità per l'utente di evitare la verifica tramite KYC (Know your Customer) e, dunque, di operare esclusivamente all'interno del sistema decentralizzato.

Nel corso del ventunesimo secolo è stato istituito il FATF, ovvero il *financial action task force*, un'organizzazione intergovernativa il cui obiettivo è evitare e disincentivare il riciclaggio di denaro e il finanziamento del terrorismo. Tale organismo ha influenzato non solo la finanza tradizionale, ma anche quell'ecosistema decentralizzato di cui ci si occupa

---

[31] KAIHUA QIN, LIYI ZHOU, YAROSLAV AFONIN, LUDOVICO LAZZARETTI, ARTHUR GERVAIS, *CeFi vs. DeFi - Comparing Centralized to Decentralized Finance*, https://www.cornell.edu/admissions/, p. 4.

nel presente elaborato. La stessa FATF, invero, delinea i concetti di VASP - fornitori di servizio di asset virtuali - e di "*travel rule*".

Il VASP è definito come entità che detiene asset degli utenti della rete e può essere inteso come un custode degli asset nella rete. è vero però che tutt'ora non si è ben delineato se il creatore delle DApps possa essere individuato come VASP, il quale darebbe responsabilità all'implementatore dell'applicazione, anche senza che quest'ultimo abbia un vero controllo sull'applicazione distribuita.

La travel rule, invece, si sostanzia in un obbligo che impone alle istituzioni finanziarie, tra cui gli appena menzionati VASP, di comunicare i dettagli univoci delle transazioni con criptovalute, comprensive di informazioni identificative. Importante è la creazione di liste nere ai fini della distruzione degli asset crittografati: nelle CeFi, data la soggezione dei soggetti a KYC e AML, le autorità possono richiedere, analizzata la situazione, di ottenere la confisca e il congelamento di asset finanziari in capo a un determinato utente. Provvedimenti quali la confisca ed il congelamento degli asset finanziari si pongono in contrasto con i principi fondamentali della finanza decentralizzata. È vero dire, però, che alcune stablecoins, come USDT e USDC, hanno già integrato contratti intelligenti con funzionalità analoghe, consentendo di conseguenza il blocco immediato di fondi e l'azzeramento del saldo per l'utente. Azioni del tipo di quelle suddette, influenzate dai movimenti normativi, possono innescare, nel contesto della finanza decentralizzata, quel fenomeno definito come *bank run*, con effetti sfavorevoli soprattutto per gli utenti che si attivano per ultimi tentando di uscire dai pool di liquidità[32].

[32] KAIHUA QIN, LIYI ZHOU, YAROSLAV AFONIN, LUDOVICO LAZZARETTI, ARTHUR GERVAIS, *CeFi vs. DeFi — Comparing Centralized to Decentralized Finance*, https://www.cornell.edu/admissions/, pp. 5-6.

CAPITOLO II
Flash loans

Ci si appresta ora a definire i cd. *Flash Loans*, paragonandoli all'istituto dell'apertura di credito in conto corrente, al fine di evidenziarne le differenze sostanziali. Non solo: verranno altresì sottolineate le opportunità e le problematiche derivanti dall'uso dei Flash Loans.

2.1 Introduzione

Nel contesto economico attuale, il progresso delle piccole e microimprese è strettamente connesso all'evoluzione costante di una nazione. Tali imprese affrontano diversi ostacoli in ragione della piccola scala aziendale nonché del sistema centralizzato limitante, soprattutto, per la bassa capacità di garantire potenziali prestiti. Esempio lampante è dato dall'operato delle banche commerciali, le quali limitano l'erogazione di prestiti alle aziende di piccola dimensione con rating di credito non elevati, tendendo a misure più conservative, e dunque creando un vuoto nel mondo finanziario.

L'emergere delle blockchain, ma soprattutto l'innovativa introduzione della finanza decentralizzata, porta a una fuoriuscita da questa situazione a senso unico. In particolare, i *Flash loans* – prestiti istantanei – si prestano a risolvere - stravolgendola - tale situazione di stallo: essi non abbassano solo la soglia di finanziamento per le microimprese, ma, in aggiunta, migliorano l'efficienza dei processi di erogazione del finanziamento, dando nuove opportunità mai viste prima. Tale modello si basa su algoritmi contrattuali cc.dd. *smart contracts* – contratti intelligenti – ovvero "una tecnologia specifica o un codice che viene memorizzato, verificato ed eseguito su una blockchain"[33] al fine di eseguire transazioni finanziarie sofisticate, tramite "copertura di leva e di liquidazione"[34].

2.2 I cc.dd. "prestiti istantanei"

I *Flash loans* sono prestiti senza collaterali, ovvero erogazione di asset digitali non garantiti, senza durata, con interessi quasi inesistenti per quanto bassi, tali prestiti vengono eseguiti da *smart contract*, basati su strutture *blockchain*, i quali erogano denaro se e solo se i fondi presi in prestito vengono restituiti con commissioni al completamento della transazione[35].

Il finanziamento viene, di regola, erogato in criptovalute, tendenzialmente stablecoin come USDC, thether, DAI, oppure ether (ETH), cryptovaluta che viene generata nella blockchain Ethereum. Sui prestiti non maturano ingenti interessi, ma commissioni, in quanto non è prestabilito un termine entro il quale il prestatore deve essere rifuso. Ulteriore aspetto del prestito, meritevole di considerazione, è l'assenza di garanzia: una volta concesso il prestito, al mutuatario non viene richiesto nessun tipo di asset come collaterale. I Flash loans, inoltre, vengono erogati da contratti intelligenti su blockchain senza autorizzazione, e ciò comporta che non vi sia un'entità di intermediazione tra

---

[33] BANCA D'ITALIA, UNIVERSITÀ CATTOLICA DEL SACRO CUORE, UNIVERSITÀ ROMA TRE, *Caratteristiche degli smart contract, p.4*

[34] XIAOLEI DING, LINGWEI ZHANG, SHUJUAN SUN, *Design of "Flash Loan" under Decentralized System,* p.1.

[35] BRAD CHANDLER, PATRICK STILES, JARED BLINKEN, *DeFi Flash Loans: What "Atomicity" Makes Possible - Toward a Comprehensive Definition of a Flash Loan,* pp. 3-4.

l'erogatore del prestito e l'utente richiedente, come tipicamente avviene, invece, per le strutture finanziarie centralizzate. Da ultimo, il capitale viene dato in prestito all'utente se e solo se vengono restituiti i fondi compresi di commissioni: in caso contrario il Flash loan viene annullato, e per effetto l'operazione si considera come mai richiesta[36].

2.2.1 L'erogazione dei cc.dd. "prestiti istantanei": le principali piattaforme

I Flash loan vengono per la prima volta introdotti nel 2019: è proprio da questa data che possiamo riscontrare un utilizzo di questi strumenti per l'ammontare di 20000 transazioni. tali strumenti trovano ampia applicazione in diversi ambiti: innanzitutto vengono comunemente utilizzati per arbitraggio, liquidazione di prestiti a margine, scambi di garanzie, e infine, non meno importante, per finanziamenti "just-in-time" riferiti a posizioni gestite da automated market maker (AMM). Tenendo presente che, come detto in precedenza, le piattaforme di erogazione di questi strumenti finanziari in un ecosistema di finanza decentralizzata sono principalmente tre: Uniswap, Aave e dYdX; di seguito viene proposta e rappresentata la liquidità dei diversi pool delle piattaforme eroganti lo strumento finanziario analizzato[37].

Protocol	Size of the Liquidity Pool	Fee to Borrowers
Uniswap v3	$1.4Bn (4 Largest Ethereum Pools)	0.05%, 0.01%, or 0.3% depending on pool
Aave	$2.0Bn (USD Coin Pool Only)	0.09%
dYdX	$251M (USDC Pool Size)	none

Figura 3: Cifre ottenute il 22/5/2022 alle 11:54 CST da Uniswap v3 (i 4 pool più grandi includono DAI / USDC $524,3MM, USDC / ETH $352,5MM, $273,3MM e WBTC / ETH $259,1MM), Aave solo dal pool di monete USD e dYdX dal pool di monete USDC.[38]

2.2.2 Il ricorso ai cc.dd. *Flash Loans*: la loro applicazione nei sistemi DeFi

Il prestito istantaneo si presta ad essere utilizzato in una pluralità di contesti: l'arbitraggio, la liquidazione, lo scambio di garanzie e il rifinanziamento.

L'arbitraggio - pratica volta alla creazione di profitto tramite la differenza di prezzo di una criptovaluta compravenduta nell'ecosistema analizzato - può essere suddivisa in tre momenti: l'accumulo di capitale sfruttando le differenze di prezzo, l'utilizzo di strategie di trading automatizzate nonché di codici a bassa latenza allo scopo di attuare tali strategie.

Liquidazione – meglio: liquidazione programmata - invece, si ha ove la garanzia dell'utente diminuisca in modo considerevole. Al fine di scongiurare tale rischio gli utenti

---

[36] *Ibid.*
[37] Ivi, p.5.
[38] BRAD CHANDLER, PATRICK STILES, JARED BLINKEN, DEFI *Flash Loans: What "Atomicity" Makes Possible - Toward a Comprehensive Definition of a Flash Loan*, p. 5.

possono utilizzare i Flash loans per auto-liquidare la garanzia suddetta, evitando eventuali perdite derivanti dall'operazione posta in essere.

Ancora: i *Flash loans* sono altresì funzionali allo scambio di garanzie. Si prenda, ad esempio, la situazione in cui un utente proceda al prestito, corrispondendo a titolo di garanzia una determinata criptovaluta: grazie all'utilizzo dei *Flash loans*, l'utente può estinguere il prestito iniziale, scambiando la garanzia con la criptovaluta da lui scelta, e, di conseguenza, richiedere un nuovo prestito. Infine, l'utente utilizza il prestito appena ottenuto per ripagare il *Flash loan*, compresi gli interessi e le spese associate laddove vi siano. Ciò consente una flessibilità mai vista in precedenza nelle operazioni finanziarie.

Da ultimo, il rifinanziamento è reso possibile solo attraverso i *Flash loans*: gli utenti possono richiedere un prestito a un tasso di interesse molto più vantaggioso rispetto a quello applicato ove ci si avvalga degli strumenti tradizionali senza dover utilizzare finanziamenti esterni, contribuendo ad ottimizzare la propria posizione nella rete[39].

2.3. I cc.dd. "prestiti istantanei" e l'apertura di credito: tratti distintivi

Interessante è raffrontare il flash loan con il diverso strumento finanziario della "apertura di credito in conto corrente".

Ai sensi dell'articolo 1842 del Codice civile "l'apertura di credito bancario è il contratto con il quale la banca si obbliga a tenere a disposizione dell'altra una somma di denaro per un dato periodo di tempo o a tempo indeterminato".

Anzitutto, dunque, l'apertura di credito – chiamato anche "fido" o "castelletto" - è un contratto consensuale, ad effetti obbligatori ed a forma libera (art 1376 c.c.). Esso potrebbe essere assimilabile al cc.dd. mutuo (1813 c.c.), anche se nel mutuo, il mutuatario diventa proprietario del denaro immediatamente, mentre nell'apertura di credito ciò accade solo dal momento dell'accredito nel conto corrente del soggetto richiedente. Ancora: il prestito istantaneo comporta interessi talmente bassi che quasi inesistenti, ma commissioni legate all'ammontare erogato; nell'apertura di credito, invece, vi sono interessi che maturano, in percentuale, in base a una provvigione stabilita alla stipula del contratto bancario. Da ultimo: le aperture di credito – a differenza dei Flash Loans – non vengono concesse con facilità, portando ad una situazione tale da impedire la possibilità di crescita - scalabilità - delle micro e piccole imprese[40].

2.4 Le anomalie nei sistemi DeFi: criticità nell'utilizzo dei Flash Loans

Veniamo ora a considerare quelli che sono i possibili attacchi che avvengono nella DeFi. Essi sono posti in essere avvalendosi degli strumenti finanziari di cui si tratta ovvero dei Flash Loans stessi utilizzati per il compimento di operazioni tali da manipolare il mercato lucrando sui ricavi ed incrementando il proprio *wallet*. Attacchi siffatti sono considerati la maggioranza negli ecosistemi DeFi: ciò per la semplicità delle modalità di attuazione e la loro capacità di sfuggire ai controlli. Tali attacchi possono essere distinti in quattro

[39] YINING XIE, XIN KANG, TIEYAN LI , CHENG-KANG CHU , HAIGUANG WANG, *Towards Secure and Trustworthy Flash Loans: A Blockchain-Based Trust Management Approac,* pp. 502-503.
[40] Brocardi, art. 1842 c.c.

categorie: *bidding up arbitrage*, manipolazione dell'*oracle machine*, attacco di rientro e vulnerabilità tecnica.

Quanto al primo tipo - *bidding up arbitrage*: esso consiste in un incremento del guadagno, derivante dalla manipolazione del calcolo del patrimonio netto. Coloro che pongono in essere tali attacchi mirano ad aumentare il prezzo del proprio asset, con l'uso del capitale altrui, per poi rivenderlo un prezzo elevato e, di conseguenza, farne profitto. Vengono presi in considerazione, principalmente, i pool delle mitragliatrici: piattaforme di prestiti, di trading affetti da leva finanziaria. Un esempio eclatante è l'attacco avvenuto il 16 febbraio 2020: bZx in solo 15 secondi, perse una somma uguale a 360.000 dollari. L'attacco si manifestò in tre diverse fasi: la prima tramite la richiesta di prestito di 10.000 ETH dalla piattaforma dYdX; dopodiché tale ammontare venne utilizzato per l'accumulo di wBTC con operazioni dedicate; infine, tramite operazioni di trading poste in essere su Bzx per trasferire l'ammontare a Kyberswap, traendo un profitto del 71%. Merita osservare come, in tale occasione, i sistemi di integrità non fossero attivi[41].

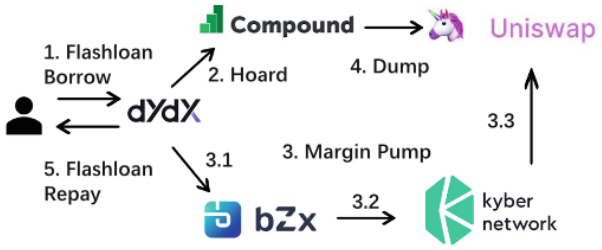

Figura 4: Offerta di arbitraggio su bZx [42]

Venendo alla manipolazione dell'*Oracle machine*: l'oracolo fornisce informazioni sui prezzi dei token in quanto la blockchain non può accedere autonomamente a informazioni esterne al proprio ecosistema. e questo se manipolato al fine di ottenere un vantaggio finanziario; si compone di due fasi principali. La prima coinvolge la raccolta dei dati esterni, come API – Application programming Interface, di prezzo o scambi centralizzati. Dati – questi ultimi - che hanno la tendenza a rispondere lentamente alle fluttuazioni dei prezzi e, talvolta richiedono, per essere trasferiti, un piccolo numero di utenti privilegiati con fiducia incondizionata per essere trasferiti. La seconda fase comporta il calcolo del prezzo medio tramite l'interrogazione della catena degli scambi decentralizzati. I dati, anche se sempre aggiornati, possono essere manipolati: esempio lampante di quanto suddetto si riscontra con riferimento alla vicenda del 25 luglio 2020. Scoperta una vulnerabilità nell'oracolo del contratto yValut sviluppato da yEarn, invero, il valore di un singolo token yVault si determinava dal rapporto del token coniati e i token depositati: nel caso di specie, per effetto di un errore nell'implementazione, si assisteva ad una incongruenza tra il cambio reale tra i token USDC e MUSD. Ciò determinava un aumento del valore di yVault, e di conseguenza, l'ottenimento di guadagni illegittimi[43].

---

[41] YINING XIE, XIN KANG , TIEYAN LI , CHENG-KANG CHU , AND HAIGUANG WANG, *Towards Secure and Trustworthy Flash Loans: A Blockchain-Based Trust Management Approach,* p. 503.
[42] YINING XIE, XIN KANG, TIEYAN LI , CHENG-KANG CHU , AND HAIGUANG WANG, *Towards Secure and Trustworthy Flash Loans: A Blockchain-Based Trust Management Approach,* p. 503.
[43] Ivi, 503-504.

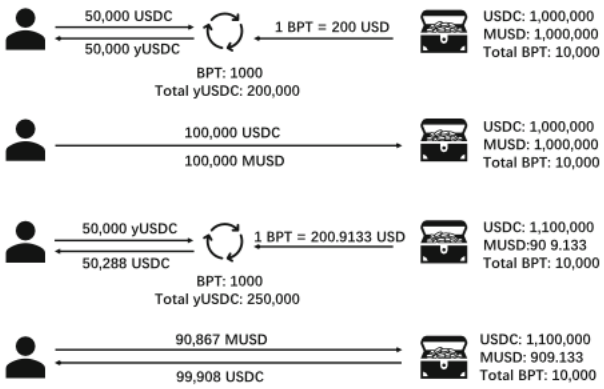

*Figura 5: mani*polazione dell'Oracle machine yVault[44]

Altra tipologia di attacco è definita "attacco di rientro": esso rappresenta una minaccia significativa nell'ambiente degli *smart contract*. Esso si manifesta allorquando un contratto esterno, maligno, assume il flusso di controllo manipolando i dati e costringendo i contratti non maligni a porre in essere comportamenti non desiderati. I contratti cd. maligni sfruttano tale situazione di "disordine" per chiamare in ripetizione una funzione specifica del contratto non maligno, al fine di accumulare token non autorizzati nel *wallet* dell'attaccante. Un esempio di un attacco del genere di quelli *de qua* si è verificato il 19 aprile 2020, sulla piattaforma Lendf.me, comportando perdite per circa 24.696.616 dollari. Sfruttando la vulnerabilità del sistema per rendere invisibile il saldo del conto dell'attaccante, si è riusciti a raddoppiare costantemente la quantità di denaro illegittimamente sottratta alla piattaforma, convertendola in BTC in diverse quantità[45].

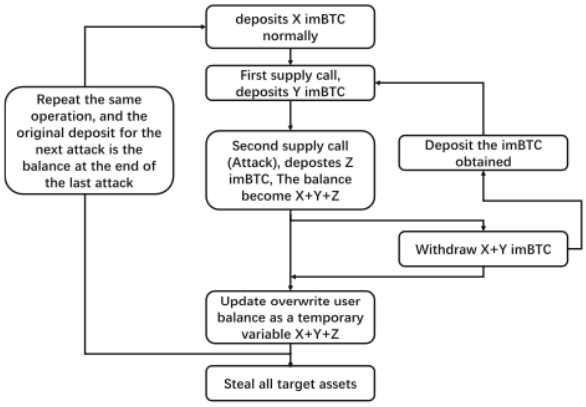

Figura 6: Vulnerabilità di rientro su Lendf.me [46]

Situazioni di vulnerabilità tecnica, infine, immediatamente riferibile alla contrattazione in uso nei mercati DeFi fa buon gioco al prelievo illecito – in quanto non visibile – di

---

[44] YINING XIE, XIN KANG, TIEYAN LI , CHENG-KANG CHU , AND HAIGUANG WANG, *Towards Secure and Trustworthy Flash Loans: A Blockchain-Based Trust Management Approach,* pp. 503-504.
[45] *Ibid*.
[46] YINING XIE, XIN KANG, TIEYAN LI , CHENG-KANG CHU , AND HAIGUANG WANG, *Towards Secure and Trustworthy Flash Loans: A Blockchain-Based Trust Management Approach,* p. 505.

token dai saldi di deposito. L'attaccante, di conseguenza, ha la possibilità di prelevare, oltre ai propri investimenti, anche quelli propri degli altri utenti[47].

[47] *Ivi*, p. 505

CAPITOLO III
L'Anomaly Detection

Prodromica alla predisposizione dei metodi di risoluzione delle anomalie nell'applicazione di strumenti finanziari quali i *Flash loans* – cui è dedicato il quarto capitolo del presente elaborato - è l'analisi dei criteri di rilevazione delle anomalie nella blockchain, quindi nella finanza decentralizzata.

Una volta delineato in maniera sommaria, il funzionamento dei sistemi di Finanza Decentralizzata, si comprende come essi possano essere oggetto di attacchi. Il che principalmente avviene per due ordini di ragioni: appropriarsi di capitale oppure acquisire popolarità all'interno della rete.

La casistica sul punto è piuttosto ampia: tra i più popolari, l'attacco – riuscito - alla rete *Bitcoin/Ethereum* nel 2017. La rete venne invasa da un numero di transazioni spam tale da bloccare il processo di verifica e, conseguentemente, da comportare ritardi nei pagamenti per 700 milioni di dollari. Non è estraneo al discorso in punto di attacchi ai sistemi DeFi, l'utilizzo dello – ormai famoso – "Schema Ponzi"; messo a punto proprio al fine di sottrarre ingenti quantità di denaro agli utenti "comuni" in cambio della promessa di considerevoli ritorni futuri.

Ciò posto, si rende pertanto necessario, al fine di evitare l'utilizzo distorto del potenziale dei sistemi di DeFi, utilizzare modelli che possano rilevare vulnerabilità e attacchi in modo tempestivo, consentendo di intraprendere azioni correttive[48]. A tal fine occorre – è importante sottolinearlo - implementare sistemi adatti e adattabili alla blockchain stessa. I modelli creati e implementati in questa rete possono, in linea di principio, essere categorizzati in base ai diversi strati della blockchain; di tal che, ad esempio, alcuni modelli sono preposti alla previsione di anomalie negli *smart contract*; altri, alla rilevazione di blocchi maligni.

La rilevazione delle anomalie è uno degli aspetti più importanti nella blockchain, se non nella finanza decentralizzata, proprio in quanto funzionale alla sicurezza sulla quale si fonda il sistema. È necessario, quindi, delineare dei modelli adatti ad operare in sistemi del tipo di quelli *de qua*; che non eguaglino quelli tradizionali, pur prendendoli ad esempio[49].

3.1 Una rapida definizione di anomalia

Un'anomalia può essere definita come una discrasia nel comportamento dell'intero set dati di un modello specifico di dati raccolti o trasmessi. Discrasia motivata da molteplici cause quali l'errore umano e non umano, ovvero attività malevoli poste in essere dagli attaccanti. La natura dell'anomalia incide sulla sua portata e, di conseguenza, sul danno derivante dalla stessa. Una transazione anomala, per esempio, può portare a un rapido decremento del prezzo di un'azione, causando crollo di mercato, così da poter essere identificata come dannosa. Nonostante il differente grado di criticità dell'anomalia, resta

[48] MUNEEB UL HASSAN, MUBASHIR HUSAIN REHMANI , *SENIOR MEMBER, IEEE,* JINJUN CHEN, *FELLOW, IEEE, Anomaly Detection in Blockchain Networks: A Comprehensive Survey,* pp. 289.
[49] *Ibid*.

comunque in ogni caso l'obiettivo di evitare che essa si manifesti e rilevarla in modo tempestivo[50].

3.2 I sistemi di rilevamento delle anomalie e la scelta del modello ottimale

Come si è detto, ai fini del rilevamento dei comportamenti insoliti nel set dati, vengono predisposti appositi modelli di monitoraggio costante dei sistemi DeFi. Questi ultimi, tipicamente, vengono progettati e suddivisi in due categorie: modelli di monitoraggio passivo e modelli di monitoraggio attivo. I primi è adoperato per il rilevamento dei dati di una parte specifica della rete al fine di identificare discrasie nella zona della blockchain analizzata; la seconda categoria di modelli si basa sul monitoraggio dell'intera rete, per identificare eventuali comportamenti anomali nel suo complesso. L'obiettivo finale è definire gli scostamenti – e il loro grado – partendo dalla normalità strutturale della rete.

La domanda da porsi è dunque quale sia il miglior modello per rilevare le anomalie ricercate. Non è errato affermare che la scelta del modello dipende dal tipo di esigenza sottostante e dal diverso scenario nel quale ci si trova ad operare, considerando che ogni situazione porta con sé vantaggi e degli svantaggi.

Per rilevare un insieme etichettato di report - se creato - il modello più consono è il modello di supervisione di apprendimento automatico; al contrario, se il set dati, cioè gli input che riceve la blockchain, sono totalmente estranei, ovvero nuovi, al modello, i modelli di apprendimento non supervisionati possono rispondere in modo più appropriato a questa situazione.

Ancora, oltre ai modelli focalizzati sui dati, importante è definire l'anomalia da ricercare: a tal fine sarebbe corretto porre in essere modelli di rilevamento degli *outlier*, come il *local outlier factor*, che circoscrive la funzione per identificare correttamente l'anomalia analizzata.

Da ultimo: l'utilizzo di modelli statistici e analitici è utile per condurre analisi approfondite in relazione alle modifiche e ai cambiamenti, sia a breve che a lungo termine, all'interno della rete.

La scelta del modello ottimale è, dunque, direttamente dipendente dal tipo di dati in input, dall'anomalia ricercata e soprattutto dall'obiettivo prefissato[51]. Di tal che, per poter gestire in maniera ottimale la rilevazione delle anomalie nella rete *blockchain*, e dunque nell'ecosistema DeFi, è importante, tempestivamente, circoscrivere il comportamento "deviato". A tal proposito, sono stati predisposti modelli di rilevamento delle anomalie in blockchain, responsabili dell'identificazione efficace ed efficiente del comportamento anomalo. Per una maggior comprensione del loro funzionamento, si suddividono i diversi modelli in sei categorie – come indicato nella Figura 3: modelli c.d. *architetture generative*, modelli basati sulla classificazione, modelli basati sul *clustering*, modelli basati sul "vicinato più vicino", modelli statistici analitici e modelli basati sul *reinforcement learning*.

[50] *Ivi*, p. 293.
[51] *Ivi*, pp. 293-294.

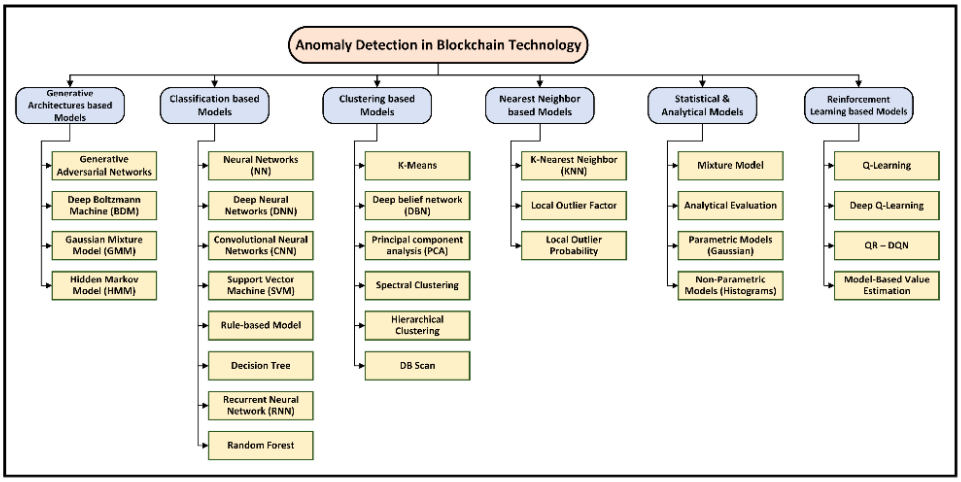

Figura 7: classificazione dei modelli di rilevamento delle anomalie nella tecnologia Blockchain. [52]

Importante evidenziare il fatto che le anomalie, riscontrate in questi sistemi, non sono generiche, poiché ogni strato della rete in considerazione si interfaccia con specifiche anomalie e il loro meccanismo di rilevamento varia a seconda del diverso livello. Ad esempio, un'anomalia definita e legata da uno "Schema Ponzi" rientra nel livello incentivante, mentre l'invio di messaggi all'interno della rete è categorizzabile nel livello di rete[53].

3.3 Le sfide tecniche per il rilevamento di un'anomalia nella rete blockchain

Nonostante – forti di una base consolidata in materia di *machine learning* - lo sviluppo di un modello per rilevare le anomalie, non sia difficile da realizzare; ove si tratti di anomalie riscontrate all'interno di un ecosistema decentralizzato, sorgono inevitabili complicazioni derivanti dalla natura stessa della rete[54]. Prima tra tutte le sfide per la realizzazione di un modello adeguato è il raggiungimento del consenso su scala di rete sull'esistenza dell'anomalia. L'ecosistema analizzato non presenta un'entità centralizzata che possa definire delle regole per identificare un'anomalia: in ragione di ciò, una volta progettato un meccanismo per rilevare gli *outliers*, esso deve ricevere l'approvazione di tutta la rete al fine di poter essere recepito come tale e ciò si complica nel momento in cui un blocco presenta un comportamento malintenzionato. Altra complicazione è data dalla necessità di selezionare accuratamente le caratteristiche delle anomalie. Blockchain, DeFi, Flash Loans sono paradigmi di ultima generazione: il che rende difficile per gli stessi ricercatori definire le caratteristiche adeguate a individuare anomalie, siano esse di entità considerevole o meno. Si rivela, ad esempio, arduo fissare in concreto lo scopo di un cd. "contratto intelligente": proprio per la difficoltà di tale procedura, si sono creati metodi automatizzati al fine di etichettare nuovi e sconosciuti contratti. Nonostante ciò, non si ravvisano differenze decisive tra le varie categorie di *smart contracts*, il che comporta il persistere di un problema di predisposizione di sistemi adeguati. Ancora: esiste un problema di programmabilità ed esecuzione del contratto intelligente a causa di vincoli ambientali. Gli smart contracts, invero, vengono sviluppati – nella maggior parte dei casi

[52] MUNEEB UL HASSAN, MUBASHIR HUSAIN REHMANI , *SENIOR MEMBER, IEEE,* JINJUN CHEN, *FELLOW, IEEE, Anomaly Detection in Blockchain Networks: A Comprehensive Survey, p. 294*
[53] *Ibid.*
[54] *Ibid.*

- in *bytecode*, anziché in codice binario: ciò comporta complessità nella realizzazione di modelli di rilevazione. In ultima istanza, mancano di regole definite: l'avvento delle applicazioni decentralizzate porta un cambiamento radicale delle regole all'interno del paradigma analizzato; causando una differenza abissale da griglia a griglia di blockchain utilizzata. Conseguentemente, una volta sviluppato un sistema di rilevamento delle anomalie su una determinata struttura, questo non potrà essere applicato universalmente, in quanto, da un lato, le regole stabilite per tale struttura potrebbero non essere applicabili ad altre tipologie, dall'altro, le regole generiche definite per determinate reti non sono adattabili a specifici settori[55].

3.4 Rilevamento degli attacchi nel nuovo paradigma

Allo scopo di identificare le sfide che gli sviluppatori devono affrontare al fine di realizzare modelli adatti alle peculiarità dei sistemi di finanza decentralizzata, rimangono da delineare le diverse tipologie di attacchi anomali che interessano tale ecosistema[56].

Prima tra tutti il rilevamento di pattern di transazione malevoli. Non a caso, le anomalie più comuni nella rete sono proprio le transazioni irregolari: a causa della pseudonimia, i nodi si sentono protetti e conseguentemente molte delle transazioni che vengono eseguite sono irregolari, poste in essere per fini malevoli. Non sono sconosciuti tentativi di riciclaggio di denaro. É necessario, pertanto, individuare la transazione prima che essa venga permanentemente registrata, al fine di dare la possibilità al modello utilizzato per la rilevazione di porre in essere le azioni idonee a porvi rimedio.

Altro è il rilevamento del double spending: come è facilmente intuibile dal nome, tale pratica è legata alla spesa o all'utilizzo di un asset più di una volta in una rete decentralizzata. Data la natura decentralizzata, e soprattutto l'assenza di un'autorità centrale preposta alla verifica delle diverse transazioni, una transazione potrebbe essere soggiogata nel processo di convalida permettendo così ai nodi malevoli di effettuare più transazioni. In tal caso, peraltro, risulta difficile procedere al rilevamento dato il forte consenso della struttura.

Altra specie di anomalia è la manipolazione di mercato: essa non è circoscritta alle sole criptovalute, ma interessa diversi fattori finanziari che possono essere compravenduti all'interno dell'ecosistema. Le principali manipolazioni di mercato – identificate dai ricercatori e dagli esperti - sono *pump* e *dump*, *wash trading* e *whale wall spoofing*. Con riferimento alla prima: un individuo, o gruppo di individui, cerca di aumentare il valore di un determinato *asset*, circoscrivendo a quest'ultimo una falsa attenzione da parte dei membri della comunità. Altra strategia è il *wash trading*: un gruppo di individui tenta di compravendere, in maniera tempestiva, criptovalute o asset allo scopo di attirare attenzione nel mercato. Tale pratica, nella maggior parte dei casi, è posta in essere in mercati fortemente deregolamentati e di piccola scala. Quanto alla manipolazione *whale wall spoofing* - tendenzialmente molto simile al *wash trading*: come suggerito dal termine inglese una "grossa balena", ovvero una entità detentrice di una somma considerevole, compra e vende nel mercato quest'ultima, traendo in inganno investitori rilevanti.

[55] Ivi, pp. 294-295.
[56] *Ibid*.

Sussunto nella categoria dei comportamenti anomali osservabili nei sistemi di finanza decentralizzata c'è il *mixing* di denaro. É necessario puntualizzare che tale processo è in sé legittimo: esso si sostanzia nella mescolanza di asset o token di diversa entità al fine di non renderli identificabili. Ciò non toglie che tale procedura venga posta in essere al fine ultimo di compiere azioni immorali, come, appunto, il riciclaggio di denaro.

Ancora: il furto, da parte degli hacker, di token degli utenti. Questo è il più comune degli attacchi avvenuti in tale rete: si parla di milioni di dollari investiti e fraudolentemente sottratti agli stakeholder di varia natura.
Gli smart contracts rappresentano un tassello centrale nell'ecosistema oggetto di studio, poiché tesi a soddisfare una funzione di programmabilità nella rete. Tali strumenti, proprio in ragione dello scopo cui sono preordinati possono essere sfruttati al fine di porre in essere attività fraudolente, come il furto di monete.

Venendo alle richieste di rete malevole: in tale rete, i nodi avversi potrebbero manipolare i valori delle transazioni prima di inviarli ai nodi pari; gli hacker, quindi, cercano di dividere la rete, al fine di non fare comunicare i nodi e potere comunicare tra di loro.
Come abbiamo precedentemente detto, nei sistemi di finanza decentralizzati, le informazioni vengono registrate in modo immutabile all'interno della struttura dati: il che implica che tali dati una volta registrati, non possono essere modificati. Proprio tale caratteristica può essere sfruttata a beneficio dell'attaccante a fini illeciti, formando una *fork* nella rete: un esempio lampante sono i bitcoin cash ovvero *fork* originati nella rete bitcoin. Gli hacker cercano, dunque, di creare percorsi alternativi per acquisire il 51% della rete, portando a conseguenze disastrose e, soprattutto, irreversibili.

Ultima – non certo per importanza - anomalia, è la manipolazione del log della blockchain. Ogniqualvolta viene compiuta una operazione rilevante – ecco la loro importanza - essa viene registrata nel registro della blockchain dal sistema dei log, al fine di certificare la qualità del prodotto. Alcuni nodi malevoli, tuttavia, potrebbero agire al fine di corrompere il log, causando un errore tale da complicare, se non rendere impossibile, la verifica audit[57].

[57] *Ivi*, pp. 295-296.

CAPITOLO IV
Casi Studio

Si ritiene possa essere utile – ed è a ciò che si intende procedere nell'ultimo capitolo del presente elaborato – soffermarsi su alcuni episodi di anomalie che hanno interessato il sistema della finanza decentralizzata, focalizzandosi sui meccanismi di attacco e frode finanziaria. Ciò al fine di prospettare di caso in caso un ipotetico modello di rilevazione adottabile di volta in volta a fini preventivi.

4.1 Attacco a BZx

Attacco noto è quello occorso su BZx – protocollo DeFi – il 15 febbraio 2020. In sostanza l'attaccante si è avvalso dello strumento finanziario Flash Loan – manipolandolo – al fine di ottenere illegittimamente profitti.

L'attacco può essere suddiviso in diverse fasi: anzitutto, l'utente si è fatto erogare 10000 ETH da dYdx e ha diviso l'importo in tre distinte parti: 5500 ETH a fini garantistici per 112 wBTC da Compound, annessi di cDAI per riscatto futuro; dopodichè, sono stati depositati 1300 ETH a margine nel vault di bZx e venduti a scoperto ETH con leva 5x, comportando operazioni di trading che coinvolgevano prestiti di ETH dal iETH di bZx e scambi su Uniswap tramite Kyber; da ultimo, l'hacker ha sfruttato le differenze tra la Uniswap e altri exchange, ottenendo 6871,413 ETH dalla conversione di 112 wBTC. Conclusa l'operazione, l'attaccante ha ottenuto ingenti quantità di criptovalute, ovvero un guadagno di 71,413 ETH, 274843,68 cETH come garanzia su Compound, posizioni aperte di 51,346 wBTC su bZx e un margine di 1300 ETH. Conseguentemente, sono stati restituiti 112 wBTC e riscattati ETH su Compound. Merita di sottolinearsi che il numero totale delle transazioni avvenute è 75: il che è, senz'altro, indicativo della portata dell'attacco.

Il successo dell'operazione si deve al fatto che le operazioni nella struttura decentralizzata sono automatizzate e basate su algoritmi prevedibili: il che consente – come di fatto è avvenuto nel caso di specie - agli hacker di prevedere e orchestrare una serie di operazioni per ottenere guadagni considerevoli[58].

4.1.1. (…): possibili rimedi

L'evento suddetto, ovvero l'attacco alla rete DeFi tramite l'utilizzo dei Flash Loans, dimostra come il sistema decentralizzato si presti ad essere soggetto ad attacchi del tipo di quello del 15 febbraio 2020. Esso, invero, è stato possibile poiché vi era un collegamento tra le varie componenti finanziarie, quali Flash Loan, piattaforma di prestiti decentralizzata, piattaforma di margin trading, router di scambio e c.d. AMM – Automated Market Maker – che hanno portato al pump-and-dump tramite lo sfruttamento del capitale preso a prestito.

Tale situazione è giustificata dalla presenza di due prerequisiti: anzitutto, l'esistenza di un AMM prevedibile, nel nostro caso Uniswap, il cui prezzo di asset sia banalmente

[58] YIXIN CAO, CHUANWEI ZOU, AND XIANFENG CHENG, Flashot: A snapshot of a flash loan attack on DeFi Ecosystem, pp. 5-6.

prevedibile e manipolabile - nel caso di specie, il prezzo è determinato da una formula di prodotto costante che convergeva al prezzo di mercato esterno, dando la possibilità all'attaccante con somme ingenti di lucrare tramite una coppia di scambi; ed, in secondo luogo, la proprietà atomica delle transazioni Flash loan, che consente di prendere a prestito ingenti somme e di restituirle nello stesso blocco di transazione; ciò consente di fare arbitraggio verso mercati esterni, senza poter rilevare le rapide differenze di prezzo che danno la possibilità al soggetto di arricchirsi. L'attaccante così riesce a creare quello che può essere definito spread. Per effetto dell'attacco il protocollo bZx ha subito ingenti perdite dovute a deprezzamento delle posizioni di *margin trading*. Non solo: anche i fornitori di liquidità Uniswap hanno subito, a loro volta, una perdita permanete a causa delle variazioni di prezzo, usate per arbitraggio e conseguente guadagno di profitto.

A porre rimedio a tale situazione può contribuire il *flashot*, ovvero un prototipo che fornisce una rappresentazione visiva dei flussi di asset e delle transazioni Flash Loan: altro non serve, dunque, che a definire come i diversi beni si muovano all'interno del sistema decentralizzato durante le transazioni[59].

4.2. Attacco a Warp finance

L'attacco di cui tratteremo prende in considerazione la piattaforma Warp finance.
L'attacco può essere scomposto in diverse fasi: in primo luogo, l'attaccante utilizzando un Flash loan, preso in prestito dalla piattaforma dYdX, ha la possibilità di ottenere una quantità elevata di DAI e wETH, senza fornire garanzie di nessun genere; dopodiché, con i fondi ricevuti, l'hacker pone in essere la frode, destinando al pool Uniswap WETH-DAI, sì da aumentare significativamente la liquidità: tramite tale operazione, si crea token LP (Liquid Pool) WETH-DAI, e cioè una garanzia tale da consentire di intraprendere altre operazioni di prestiti di token. Momento cruciale dell'attacco consiste nella manipolazione del prezzo dei token creati, ossia LP: il che avviene nel momento in cui l'attaccante esegue una serie di scambi e forniture di liquidità strategicamente all'interno del pool sopracitato; conseguenza è l'aumento significativo di wETH nel pool, e, dunque, del prezzo del token LP. Questa manipolazione è stata possibile tramite diverse operazioni di trading. Il limite di prestito, su Warp finance, è calcolato sulla base del valore dei token LP forniti a fini garantistici: di conseguenza, l'utente malintenzionato procede alla manipolazione del prestito massimizzando il valore del token; il che gli consente di prendere in prestito una quantità maggiore di token illegittimamente. Per completare l'attacco, l'hacker ha ripagato i prestiti istantanei ottenuti inizialmente, utilizzando i DAI derivanti dagli scambi per ripagare parte dei DAI; tuttavia, non aveva abbastanza wEth per ripagare il Weth, quindi, per coprire il prestito di WETH, ha scambiato tutti i DAI rimanenti in proprio possesso con WETH dal pool Uniswap da lui manipolato, al fine di completare il rimborso e ottenere notevoli profitti da Warp Finance, causando danni al sistema decentralizzato per circa 8 milioni di dollari[60].

4.2.1 (…): possibili rimedi

---

[59] *Ibi*.
[60] WARODOM WERAPUN, PAWITA BOONRAT , TANAKORN KARODE , TANWA ARPORNTHIP , JAKAPAN SUABOOT , ESTHER SANGIAMKUL, *The Flash Loan Attack Analysis (FAA) Framework—A Case Study of the Warp Finance Exploitation,* pp. 10-11.

Stando così le cose, diversi studi si sono posti come obiettivo quello di approntare una soluzione alle problematiche di rilevamento e di prevenzione degli *exploit*.

Uno dei modelli da tenere in considerazione è definito *fair reserve model* ovvero modello delle "riserve eque". Esso si basa sulla determinazione dei token che vengono generati, LP, utilizzando riserve medie ponderate nel tempo, c.d. TWAR. Il pregio del modello suddetto sta nel fatto che esso non si basa sulla fluttuazione di breve periodo, bensì prende in considerazione le variazioni del lungo termine e, a differenza del modello di Warp Finance che utilizza riserve in tempo reale, è meno manipolabile in relazione ai token LP causati dal prestito istantaneo. Altro risultato significativo è che, tramite l'utilizzo del suddetto modello, il danno derivante da un eventuale attacco è pari a zero. Quest'ultimo è un passaggio non di poco conto in quanto si desume che l'applicazione di tale modello possa prevenire l'exploit nella sua interezza. Essendo il danno proporzionale al prestito concesso all'utente malintenzionato, il modello de qua impedisce, appunto, l'aumento della dimensione del prestito, creando un grande contrasto contro il modello tradizionale. Il danno, peraltro, può variare in base alle dimensioni delle riserve della piattaforma: in scenari di offerta illimitata, il danno è proporzionale al prestito; tuttavia, in scenari di offerta limitata, il danno nella piattaforma può essere influenzato da altri fattori.

Di conseguenza, il modello è un modo efficace per rilevare e combatter gli attacchi di manipolazione dei prezzi in futuro. Poiché è immune alle fluttuazioni di breve periodo e ha la capacità di prevenire significativamente i danni, apporterebbe un vantaggio significativo ai sistemi di finanza decentralizzata, rendendoli più solidi per future operazioni finanziarie[61].

4.3 Attacco a Harvest finance

L'attacco di Harvest è un'altra tipologia di flpattack ovvero un attacco tramite Flash Loan. L'attaccante, tramite una serie di acquisti e vendite di token, riesce a generare significativi guadagni. L'attacco segue uno schema definito "Multi-Round Buying and Selling" (MBS): in prima battuta, l'agente malintenzionato guadagna una ingente somma di denaro tramite l'erogazione di una quantità di USDC da Uniswap, mediante la quale può iniziare il processo di frode. Successivamente, nel round di acquisto, il soggetto compravende il capitale acquisito di USDC in fUSDC: tramite questa operazione dove si acquista costantemente il bene, fUSDC, tramite la compravendita dell'asset erogato grazie al Flash Loan, esso sale costantemente, creando ingenti guadagni in capo all'hacker. A questo punto, si apre la fase di vendita: innalzato il prezzo di fUSDC, questo è venduto dall'utente a un prezzo maggiorato, creando un profitto considerevole a proprio favore. Tale processo viene ripetuto in maniera costante, originando un ciclo di acquisto, aumento del prezzo e vendita; con conseguente guadagno costante in ogni round avvenuto. Nel caso di specie, ciò è stato favorito dalla manipolazione del prezzo, ma anche dallo sfruttamento del protocollo Harvest Finance.

Al termine dell'operazione, dunque, l'attaccante ottiene una quantità di denaro consistente, a riprova del fatto che due fattori, manipolazione e sfruttamento all'interno

[61] *Ivi*, pp. 11-13

del protocollo DeFi, possono portare a illegittimi profitti, sottolineando, dunque, la necessità di applicare modelli di mitigazione e prevenzione[62].

4.3.1 (…): possibili rimedi

Una possibile soluzione è stata ipotizzata, tramite la creazione di LeiShen - modello ottimale per la rilevazione degli attacchi tramite Flash Loans. Il modello opera principalmente in tre fasi: nella prima fase, il modello identifica le transazioni di Flash Loans nelle principali piattaforme di erogazione (Uniswap, AAVE, dYdX), tramite le funzioni chiamate e i log associati a quella piattaforma; nella seconda, si tratta di rendere comprensibili gli asset trasferiti, in quanto, inizialmente, tutti gli account sono rappresentati come indirizzi Ethereum e la relazione con le applicazioni DeFi è sconosciuta. Tale fase, a sua volta, è articolata in due step: la prima ovvero l'etichettatura dell'account, in quanto LeiShen riesce ad associare nomi di applicazioni DeFi agli account, in modo da poterli identificare più facilmente. Gli account sconosciuti vengono etichettati con il nome dell'applicazione precedente, se ciò non è possibile con l'indirizzo del nodo radice nell'albero di relazione. La seconda fase è relativa alla semplificazione dei trasferimenti, al fine di cancellare tra le applicazioni prese in considerazione le operazioni ridondanti e unire quelle correlate. La terza e ultima fase - più operativa - consiste nell'identificazione del modello di attacco, tramite i tre fattori chiave ovvero lo scambio, la creazione di liquidità e la rimozione di quest'ultima. Obiettivo è rilevare l'operazione di scambio, definendo condizioni specifiche che si basano, infatti, sui trasferimenti di asset in capo agli utenti[63].

Risulta evidente il potenziale di tale modello: innanzitutto, tra le principali caratteristiche di *LeiShen*, vi è la sua capacità nel rilevare *flpattacks* noti e no. Capacità che potrebbe essere implementata al fine di monitorare costantemente le transazioni e rilevare le operazioni sospette all'interno della rete, agendo preventivamente. Una volta rilevate – qui entra in gioco un'altra funzione - si tratta di definire le difese più appropriate al fine di mitigare il costante utilizzo di Flash loan a fini illeciti. Ancora, la rilevazione dell'attacco avviene in tempo reale, in modo da consentire a *Harvest* di reagire a ipotetiche situazioni di emergenza, sospendendo temporaneamente le transazioni o intraprendendo azioni correttive.

In ultimo è a parere di chi scrive utile implementare l'uso di tale modello di rilevazione anche allo scopo incrementare la consapevolezza della comunità sugli attacchi che avvengono in questa rete, al fine di poter, autonomamente, agire di conseguenza[64].

---

[62] QING XIA, ZHIRONG HUANG, WENSHENG DOU, YAFENG ZHANG, FENGJUN ZHANG, GENG LIANG, CHUN ZUO, *detecting flash loan based attacks in Ethereum,* p. 157.
[63] *Ivi*, p.158.
[64] *Ivi*, pp. 161-162.

Conclusioni

La Finanza Decentralizzata (DeFi) offre, come si è potuto constatare, vantaggi senza precedenti. Tuttavia, la serie di attacchi avvenuti sfruttando lo strumento finanziario Flash Loan, ha contribuito all'emersione delle criticità insite in questo ecosistema.

Nel quarto e ultimo capitolo – dedicato agli attacchi avvenuti nelle diverse piattaforme DeFi- si è evidenziato come si possano manipolare i Flash Loans, sì da consentire attacchi posti in essere sfruttando falle nei diversi protocolli, tali da generare notevole profitto in capo agli utenti malintenzionati e a discapito della sicurezza del sistema. Proprio per questo, dopo un'analisi degli attacchi che hanno interessato *Bzx*, *Warp finance* e *Harvest finance*, emerge la necessità di implementare dei modelli di rilevazione delle anomalie finalizzati alla difesa e alla mitigazione di exploit di vario genere.

Come abbiamo visto, i diversi modelli proposti, quali *Fair Reserve Model* e *LeiShen*, per la rilevazione di attacchi tramite Flash Loans si sono rivelati promettenti al fine di migliorare la sicurezza nei protocolli DeFi, rendendo il sistema più resistente a future situazioni da parte di soggetti con intenzioni illegittime.

Nonostante ciò, è vero dire che per quante soluzioni si cerchi di delineare, il nuovo paradigma è in costante evoluzione, di conseguenza vi è bisogno, al fine di affrontare al meglio le sfide future, di un atteggiamento proattivo, che coinvolga sia gli utenti della rete, sia gli sviluppatori, al fine di creare una sicurezza efficace ed efficiente senza precedenti.

La collaborazione di esperti e informatici potrebbe portare a sviluppare protocolli DeFi, modelli, strumenti finalizzati alla protezione dell'integrità dell'ecosistema analizzato, non solo tramite l'aumento degli standard di sicurezza informatica, ma anche tramite uno sviluppo sostenibile del concetto più ampio di Finanza Decentralizzata.

Il fine ultimo è, dunque, assicurare agli utenti della rete livelli consoni alla detenzione di asset di vario genere, per aumentare la scalabilità e l'utilizzo di questo nuovo paradigma senza intermediazione e incrementando la fiducia di investitori, sviluppatori e singoli soggetti che vogliono essere indipendenti da sistemi tradizionali, come per esempio l'istituzione bancaria. L'implementazione di modelli di rilevamento delle anomalie, quindi, rappresenta solo un primo step di un lungo percorso finalizzato ad assicurare trasparenza, resistenza, efficacia ed efficienza al concetto di Finanza Decentralizzata.