Article

Terra Luna and the Future of Internet Investments: Towards a Framework for Investors' Protections

Dimitar Kyosev[1], Dimitar Anastasovski[2]*, Mirko Kikovic[3] and Orfefs Voutyras[4]

[1] Alis Grave Nil, Next Generation Internet (NGI) Program; kyosev.dimitar@gmail.com
[2] Infideo, NGI; dimitaranastasovski@yahoo.com
[3] Infideo, NGI; mirkokikovic@gmail.com
[4] National Technical University of Athens; o.voutyras@gmail.com
* Correspondence: dimitaranastasovski@yahoo.com

Abstract: This article presents the results of a cross-disciplinary applied study exploring investors' protections in the context of distributed ledger technology (DLT) smart contracts. Fusing legal, business, and technical perspectives, we developed a framework for protection from non-commercial risks for stablecoins, taking advantage of DLT and AI. A key concept we propose is the monitoring of disinformation and fake news to prevent malicious parties from abusing our solution. Based on the similarities between central bank digital currencies (CBDCs) and stablecoins, we propose scaling up our results to all future internet investments performed without face-to-face contact between the investor and the company.

Keywords: cross-disciplinary; AI; blockchain; investment; protection

1. Introduction

In May 2022, the exchange value of the Terra Luna stablecoin collapsed by over 99%, wiping out most of USD 60 billion worth of investment. At the time of writing, the price is just EUR 0.00001 compared with over EUR 100 at its height. The collapse puts the spotlight on the protection of investors in stablecoins and how to ensure their financial interests more adequately. This is the main topic of this article. Here, we review the academic literature and the scientific debate over stablecoins, investors' protections, and the utilization of DLT. This will be of great importance for the rollover of central bank digital currency (CBDC) in this decade, determining the future of internet investments.

The issue of stablecoins has received considerable attention in recent years from numerous academics. Here, we will cover just a small fraction of the literature, to emphasize the main trends and ideas in the scientific community concerning the topic.

Some authors, such as Chohan (2019) [1], have stressed the fundamental difficulties of constructing pegs to traditional currencies. He argues that those difficulties are not tackled by stablecoins. Adding to the voices of concern are authors such as Doerr et al. (2021) [2], who argue that "If DeFi were to become widespread, its vulnerabilities might undermine financial stability. These can be severe because of high leverage, liquidity mismatches, built-in interconnectedness, and the lack of shock absorbers such as banks. Existing governance mechanisms in DeFi would provide natural reference points for authorities in addressing issues related to financial stability, investor protection and illicit activities."

This rather dim assessment is countered by some authors, such as Picard (2021) [3], Dhar (2020) [4], or Cao (2021) [5]. They argue that there is a genuine benefit to using decentralized finance and stablecoins to reduce volatility. Cao et al. (2021) [5] stated that "Stable coins are useful for reducing volatility and providing alternative investment medium". For Dhar (2020) [4], stablecoins may fuel private-led decentralized growth across borders, and with appropriate stakeholder coordination, could protect privacy and enable regulated data protection.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

Different nuanced opinions highlight certain behavioral elements of stablecoins. Wang et al. (2020) [6] observed that "the safe haven property of stablecoins changes across market condition". Moreover, it would appear that stablecoin returns, volatility, and volumes are highly correlated with corresponding Bitcoin time-series, making stablecoins important contributors to systemic uncertainty (Hoang and Baur, 2021 [7]).

The issue at the center of our research—the protection of stablecoin investors—also attracts attention from academicians. Picard (2021) [3] called for the protection of investors through the segregation of accounts and insurance schemes. Arner and Frost (2020) [8] called for the embedding of supervisory requirements into stablecoins to prevent abuse. Kampakis (2022) [9] proposed the idea of using tokenomics audits to provide some indication of investor risk. Dynamic stablecoins monitoring through indexes and other technical parameters that could be hardwired or audited independently is an idea championed by Choi (2022) [10]. Looking from the enforcement perspective, Nøkleholm and Kviseth (2021) [11] emphasized that regulating stablecoins is challenging, and protection for investors may be difficult to enforce.

Hemenway and Hammer (2022) [12] made a brilliant observation on the causes for Tera Luna collapse and stablecoins in a broader perspective: "For example, many stablecoins maintain the ability to prevent redemption of tokens for fiat money ("freezing"), retrieve tokens without consent ("clawbacks"), or even unilaterally block certain digital wallet addresses from transacting ("blocklisting"). Most or all stablecoins set forth no formal procedure for how these decisions are made, leading to concerns that they are non-transparent or even arbitrary. In addition, stablecoins frequently change their online disclosures (if any) and limited terms of service, without providing notice to stablecoin users. The use of limited terms of service combined with extreme practices in the stablecoin space raises significant questions regarding stablecoin behavior and user accessibility, as well as the validity and enforcement of contracts of adhesion and consumer protection. Additionally, these activities have implications for credit, liquidity, and operations, as well as financial stability."

Staying with Terra Luna, Uhlig (2022) [13] found that the majority of UST coin holders waited until the probability of suspension was rather high before deciding to burn their holdings. This emphasizes the issue of investors' vulnerability: particularly retail investors.

There are quite a few valuable academic contributions concerning the importance and methods of protecting investors from an economic perspective. We will visit just a few of them to provide the reader with a general framework of the economic debate on this issue.

As established in the economic literature, the protection of investors is critical for both economic growth a more equal income distribution (Greenlaw and Shapiro, 2017 [14]). Put simply, if investors cannot extend credit to corporations on relatively safe terms, the latter will not have the resources to create economic growth, whereas the former will be unable to earn interest on their capital. Therefore, creating a system where investment can flow to innovative companies and projects (such as stablecoins) is especially important (Reinert, 2007 [15]), even more so in the context of central bank digital currencies (CBDCs) which will change the way internet is used to facilitate investments and the extension of credit (Auer, 2020 [16]).

This position is well established, and numerous jurisdictions—including the EU—are providing legally binding protections for investors (Gugler, 2004 [17]; Asril, 2019 [18]). However, when referring to DLT assets, those protections are watered down (Mokhtarian, 2018 [19]). The main issues are the cross-border nature of financial transfers and the technical specificities of the new technology.

What our proposition also takes into consideration is the role of social media and its impact on investors' relationships. As already established in the literature (Snow, 2015 [20]; Mikołajewicz-Woźniak, 2017 [21]) social media is beginning to play a key role in investors' relations, especially with retail investors. Social media is a serious mover in the market, because investors have cognitive shortcomings (Black, 2012 [22]) and their

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

behavior is shaped by rumors and sometimes unrealistic expectations (Costola, 2021 [23]). Therefore, social media is known to disrupt markets and stock valuations.

This study explored various protection tools, including new forms of transparency and investors' actions enabled by DLT. It is empirically established (O'Connor, 2014 [24]) that more transparently governed companies perform better for investors (their share price is significantly higher). Blockchain can increase the security of investors and provide additional tools for all stakeholders to maximize their outcome simultaneously (Zhu, 2016 [25]). Therefore, our research assessed the practical implementation pathways for such DLT-based tools.

In this study, we relied on the common features of smart contracts across platforms (Polge, 2021 [26]; Shi, 2021 [27]). Despite the differences in consensus creation, and some performance issues, the core architecture of the smart contracts can be transferred on various platforms. In other words, as long as the underlying business case (protection for investors) is clearly researched, it would be possible to design smart contracts with similar outcomes in all platforms (Polge, 2021 [26]; Kuo, 2019 [28]).

This debate of investor's protections for stablecoin holders is extremely important because CBDCs share many communalities with stablecoins. This puts investors' protection in a strict cross-border situation: a position where the regulatory and technological boundaries are unclear. Considering advanced solutions will benefit trust creation, transaction certainty, and the wider economy.

2. Materials and Methods

In this article, we explore the problem that was emphasized in the above literature review—and the collapse of Terra Luna—concerning the protections on which investors in stablecoins can rely. We utilized the methods of evaluative research (Babbie, 2007 [29]), where we designed a solution framework, performed experiments (simulation), and compared the results with the fallout of Terra Luna.

Formulating the problem represents the first important methodological task. In this regard, we considered two elements. Firstly, the protection of investors is not carried out in a single action, but is the systematic observation of rules that lead to actionable conditions. Secondly, as noted in the literature (see, among others, Giannetti, 2010 [30]; Asril, 2019 [18]), investors' protection is not to protect them from trade risks, but from unfair, fraudulent activities or actions in gross negligence. In that line of thought, our research question concentrated on formulating a framework for investors' protections that would empower investors in stablecoins to protect themselves from non-commercial risks.

The utilization of AI and smart contracts in the solution was also an element of our research question, because both have significant potential to be implemented in the stablecoin setting. The scaling up and automation abilities for those technologies and their integrated implementation are a strong indicator we should consider them as an element of the suggested framework.

Therefore, we can define our research question as follows: "How to design a framework for protection from non-commercial risks for stable coins, taking advantage of DLT and AI?". Obviously, answering that question would require us to compare the existing protections for those investors with the protections we propose.

The methodology of this analysis was based on three main metrics for the protection framework we identified: time, costs, and availability. The first aspect refers to the time required for all the steps of the procedure from initiation to resolution to be completed. Cost as a metric refers to the monetary value of the said measures from the perspective of the investor (user). The availability metric refers to the chance that the investor will achieve a satisfactory outcome from the protection proceedings, where the satisfactory outcome is defined as the recouping of all costs from financially unfavorable event to the holdings of the stablecoin investor.

The experimental setup and evaluation were the last elements of the methodology. The experiment will demonstrate the indicative power of AI analysis of social media. The

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

evaluation was based on probabilistic estimates of the detection of correlations between increased false news deriving from stablecoins in trouble (e.g., Terra Luna) and their subsequent collapse.

3. Results

3.1. The Legal Perspective

There are numerous stablecoin projects across various jurisdictions, where the dispute resolution process might be settled outside of the project's residence jurisdiction. However, various existing and upcoming regulations may delegate the responsibility to oversee and enforce investors' protection, even towards non-domicile projects, to government agencies—such as the SEC, ESMA, or CFTC.

This rather complex analytical background calls for a more abstract approach, where we will take each option by itself to determine the ramifications for investors' protection. After that, we take stock of the possible mix of each issue.

The framework for our analysis had the following structure (see the table below):

1. Investors protections: those include the various actions that stablecoin holders take or are taken on their behalf to ensure that their financial interests are considered in the process of stablecoin management and operations.
    (a) Statutory for citizens/residents only of the domicile jurisdiction: these are the protections of the financial interests of investors that are provided to them by legally binding rules made by a legislator, or another rule-setting administrative body, and are only territorially binding:
        (i) Weak protections are protections where the coin holders rely on a third party to protect their rights—this includes regulatory bodies (e.g., license review) or the internal procedures of the coin administrator.
        (ii) Strong protections (including external arbitrage, fiduciary duties, etc.) are based on actions that investors can perform to individually protect their own interests.
    (b) Statutory for all stablecoin holders are the protections granted by law to every investor regardless of their citizenship or domicile status.
    (c) General Terms and Conditions protections:
        (i) Weak protections as defined here are the protections provided singularly by the administrator, which suggests lower actual availability;
        (ii) Strong protections in this context refer only to arbitrage actions, which are agreed contractually between the parties;
        (iii) Protections based on voluntary standards are hardwired protections that can be automatically or semi-automatically triggered.
2. Dispute resolution is a method of reaching outcomes for a dispute and the enforcement of that outcome:
    (a) Amicable resolutions occur when the administrator and coin holder agree on a specific action;
    (b) Statutory mediation/resolution authority (e.g., CFTC) resolution is based on an administrative body which is tasked with regulating the administrator or protecting the investors;
    (c) Arbitrage resolutions refer to all kinds of out-of-court procedures that have been agreed by stablecoin users and the administrator:
        (i) Cost, time, and access—these relate to the monetary costs and time of arbitrage actions;
        (ii) Enforceability of the award is an issue which is directly related to the availability of this particular remedy. Notably, the enforceability of arbitrage awards occurs through the court system unless the parties decide to comply voluntarily;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

(iii) Relation of the ruling with the policy of the administrator is the final point that should be assessed in relation to our systemic analysis here, because it would indicate whether permanently changing the administrators' terms would result from arbitrage case-law.

(d) Court process is a dispute resolution performed through the judicial system of the domicile jurisdiction for the stablecoin and/or its administrator. In this analysis, we assumed this to be one and the same, and we did not explore possible conflicts of law in cases of different domiciles of the administrator or the stablecoin project.

(e) Automated protections (new generation of smart contract protections promoted by OttCT):

(i) Triggering conditions refer to the availability of the remedy under specific conditions;

(ii) On/off chain transition is the property for a specific action on the chain to be binding off the chain as well. This property increases the availability of the dispute remedy, as well as its transparency;

(iii) Automated enforcement is an inherent element of smart contracts. It provides highly structured and predictable outcomes of specific unambiguous conditions, increasing the availability;

(iv) Cost and time refer to the incurred financial payments made by investors and the speed for the resolution mechanism to be enacted.

Table 1 provides an overview of the analysis we performed under three criteria—cost, time, and availability. The three criteria summarize the actual expectation that an unsophisticated investor will be able to successfully press their rights through the described means.

This analysis considered both weak and strong protections as low in availability. When referring to weak protections, by definition these are based on the will of third parties (the administrator or regulators) to act on behalf of the investor. In this sense, the actions of the administrator are (based on historical evidence) unlikely to redeem to significant amount of any financial loss the investor may suffer. On the other hand, actions by regulators in principle (and by referring to their record in the stablecoins context) are punitive for the administrator; however, penalties are not meant to redeem any losses that individual investors may have suffered. The strong protections—those based on an arbitration or court judgment—have intrinsic barriers: high costs and a relatively low time for the award to be decided. Arbitrages usually only award partial cost covering, which hugely diminishes the interest in arbitrage judgment. In some jurisdictions, the costs for legal counsel are carried by each side, which is also detrimental for remedy availability for small investors. Moreover, enforcement of the court/arbitrage decision is a complete process which assumes there would be sufficient assets available to the administrator. The recent history of stablecoin collapses (e.g., Terra Luna) suggests that this is unfounded assumption. All these reasons would make the availability of strong protections rather low in actuality. A retail investor by themself would not be able to adequately protect their rights, because the time, costs, and procedural involvement are prohibitively high.

On the other hand, automated or semi-automated protections are rated high on the availability scale because the chances of the investor achieving satisfactory outcomes are, by design, high—specific tools allow for swift actions made by the administrator or the investors to protect the collateral (e.g., suspension of trade) or to orderly oversee different elements of the unwinding procedure (e.g., the appointment of questors, collateral sale, etc.). Those procedures, naturally, should be followed in an off-chain/on-chain event coordination. The issue of possible liability of the investors in the above-mentioned procedures is considered in detail subsequently.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

Table 1. Evaluation of legal protections.

Legal Type Protections		Strength of Protections	Resolution	PREREQUISITES*		
				Cost	**Time**	**Availability**
Statutory Rights	for Citizens	WEAK	Amicable Resolution	Very Low	Very Fast	Low
			Mediation	Very Low	Fast	Low
		STRONG	Mediation	Very Low	Fast	Low
			Arbitrage	High	Medium	Low
			Court Proceedings	Very High	Very Slow	Low
	for Non-Citizen	WEAK	Amicable Resolution	Very Low	Very Fast	Low
			Mediation	Low	Fast/Medium	Very Low
		STRONG	Mediation	Low	Medium	Very Low
			Arbitrage	High	Medium	Low
			Court Proceedings	Very High	Very Slow	Very Low
Rights under General Terms and Conditions	for All	WEAK	Amicable Resolution	Very Low	Very Fast	Low
			Mediation	Low	Fast	Very Low
		STRONG	Arbitrage	High	Medium	Low
		AUTOMATED	Oracle	Very Low	Very Fast	Very High
			Group Action	Low	Very Fast	High
*definitions and descriptions of the fields of the table are provided within the text						

Automated and semi-automated protections would be legally introduced in the General Terms and Conditions (or other binding contractual agreement); therefore, their scope can range beyond and above the statutory rights guaranteed by the local jurisdiction.

3.2. The Business Perspective

The search for a framework would not be complete if the financial incentives of the stakeholders were not considered. A protection framework would need to take into account the motivation for its own implementation, market roll-out, and difficulties. This is a pre-condition for technical development, and we should mention the help that we received in this tangent of our research from TruBlo and NGI Tetra. We reviewed the business perspective using the functional investor protection framework. For convenience and to reduce space, we label that framework OttCT (On to the Chain Trustworthy).

3.2.1. Additional Checks by Investors

Building upon the need for real-time checks, we assessed the customer experience through investors' engagement that reduces fear, uncertainty, and doubt (FUD). With a plethora of possibilities, all residing on data insights and analysis, we developed the grounds for innovation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

The financial benefits, in addition to the promotional value, tend to create repeated engagement by companies. Moreover, we researched the method where companies can gain significant value for the future by involving the gamification model and holding the dedicated tokens.

3.2.2. Business Model

From the business perspective, we should also pay attention to the sustainability of the business model. Our research was also value-based, conducted within the network of NGI TruBlo and with the support of EU taxpayers. In the proposed framework, we integrated investor protections and the concept for open-source solutions. In this respect, it is worth exploring how those business models can be economically viable in more detail.

Choosing an open-source model is a viable option due to the importance of developing this solution for the overall community. Investors' protections have the potential to drive the economy in spheres that are neglected by some traditional investors, such as cryptocurrencies and impact investing. Both spheres tackle questions that can positively and negatively influence companies (and industries); therefore, peer reviews, contributions, and improvements are of utmost importance.

In analyses of business models, as a template to define the business plan, we considered the applicability of the four different cases in researching the possibility of a self-sustaining business model:

1. Support services for the platform;
2. Dual licensing strategy;
3. "Open core" licensing model;
4. Leverage to sell other products and services.

3.2.3. The Business Potential for OttCT

Considering the abovementioned business models, there is a possibility of using several cases to achieve a sustainable solution. The reason is also mentioned in the context of solving real problems in the specified niche (stablecoins initially, or subsequent impacts on investing and other use cases) and the technical savviness of the contributors (such as developers' blockchain communities). These two reasons are prerequisites for the success of the solution.

3.2.4. Evaluation

We evaluated the business advantages and financial incentive alignment in regard to the methodology described in the Materials and Methods section. Therefore, we should define what the metrics denote in the context of the business perspective.

Cost as a metric refers to the monetary value of the measures from the perspective of the investor (user). More specifically, from the business perspective, this metric is the cost of adopting the proposed protection framework, based on initial projections. Time as a metric refers to the time required for all steps of the procedure, from initiation to resolution, to be completed. The time measure more specifically operationalized here is the time taken for communication (from the company to the investors) and reaction (by the investors). As mentioned above (see Methodology), the availability metric refers to the chances that the investor will achieve a satisfactory outcome from the protection proceedings. In the context of the business perspective, this is the ability of companies to raise capital and for investors to remedy their concerns. The latter two are in obvious correlation. We also tested this correlation with in-depth interviews with investors and found it to hold rather robustly.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

Table 2. Evaluation of business incentives.

	Incentives for Companies		Incentives for Investors	
	Current	OttCT	Current	OttCT
Cost	Very low	Medium	Very Low	Low
Time	Medium	Very low	High	Low
Availability	Low	Medium	Very low	High

Based on Table 2, as a business case, we could make pretty strong argument that the OttCT solution is superior to the current situation.

3.3. AI for Transparency and Building Trust through the Analysis of Social Media

3.3.1. The Need for Building Trust and Social Media Analysis

The OttCT has been assessing trust-building on the one hand as a continuous process, and on the other hand as a probabilistic measure. We describe this dual view in a bit more detail, where, by narrowing our focus, we will put the emphasis on stablecoins.

Systemic consistency in the outcomes—in our case, investment in a stablecoin, which would stay stable (unlike Terra Luna, for instance)—is a process. There are algorithmic steps where investors' money is turned into underlying assets, and those assets perform until the redemption of support, and the stablecoin's peg is maintained. The balance is not a given (as recently made painfully obvious), and active measures must constantly be taken to preserve the stability of the assets. Therefore, trust in stablecoins is based on the continuous ability of the crypto asset to perform, which is a process of reinforcement.

The second element of trust is its probabilistic nature. The probability of a certain event coming to pass increases with the active steps taken towards its completion, and decreases otherwise. Similarly, the likelihood for consistency of the desired outcome—maintaining the peg crypto-fiat/crypto-commodity—is greatly increased should the interested parties (investors) have active revenues to address any grievances. Naturally, as everyone involved understands, a high probability does not equal certainty. Blockchain can hugely increase trust between the parties, mitigate risks, and reduce the chances of misbehavior; however, it will not create absolute certainty.

In this context, the proposed task, with valuable assistance from TruBlo, was to increase the probability of the main performing indicator of stablecoins—maintaining their peg. To that end, we underwent the processes stablecoins put in place to ensure continuous convertibility. In those processes, we identified key flux points—on-chain/off-chain interactions—and have developed a framework to monitor and remedy any infringements. Our solution, in essence, could allow for automatic monitoring and rapid, actionable recourse should the delicate balance of the stablecoin stray off-course.

3.3.2. Security Framework

We did not envision building the blockchain from scratch, but instead used the service as it was; therefore, security came by design. However, we address some of the possible attacks and how to prepare our system to respond to and mitigate them.

One of the weakest points in the blockchain is smart contracts. The majority of hacks and exploits result directly from this vulnerability. The security of smart contracts strictly relies on the coding skills of whoever writes them. To enforce this weak point, we discuss the features of a draft smart contract that would satisfy the compliance for a secure smart contract, as well as any contract which should be audited for additional safety. This conceptual draft contract should be only editable on certain points where the possibility to be exploited will be minimal.

The possible malicious actor identified in our system was the user themself. We considered mitigation measures for #Sybil Attack and # 51% Attack. Furthermore, we utilized #Amazon CloudFront.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

3.3.3. Initial Prototype

Our initial prototype consisted of two docker containers that were running and communicating with each other. One of the containers was responsible for pulling the information inserted by the client and passing that information to the second container, which was responsible for giving results based on client input.

In our dataset, we collected approximately 23,000 binary-classified tweets (real/fake), from two different sources (GossipCop ~ 22k, PolitiFact ~ 1k), using FakeNewsNet. Our data were unbalanced: 75% were real, and 25% were fake news (see Figure 1).

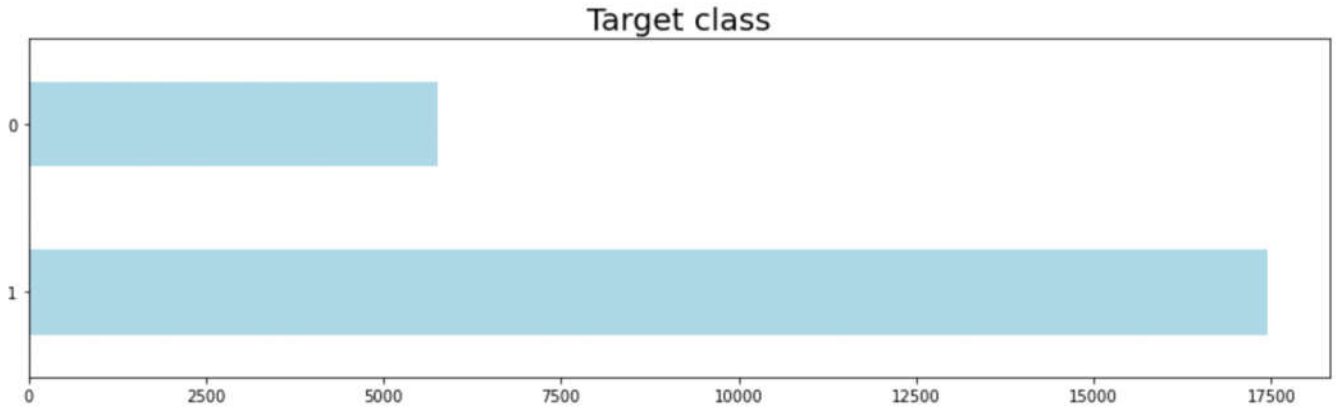

Figure 1. Target CLASS.

In further enhancements, we could collect additional data, for both fake and real categories.

Text Preprocessing and Data Split

Many different techniques can be used for preprocessing text, including lowercasing, keeping only alphanumerical values, stemming words, lemmatizing words, removing stopwords, etc. Specifically, in our case, those steps could eliminate important differences between fake and real tweets. For the pilot version, we achieved the best results when we only applied lowercasing.

In later versions, we could apply the abovementioned techniques on specific portions of the data. The dataset was not too large; thus, we split it into training and testing sets in a ratio of 80:20. In addition, we stratified the data by target value.

Count Vectorizer

A Count Vectorizer machine faces difficulties when handling raw text; therefore, the goal was to transform text into numbers and use these numbers as inputs for the algorithm. CountVect converts a collection of text documents to a vector matrix. First, a vocabulary of all words is derived; then, the words are sorted and assigned an ordinal number. The sentence is represented as a vector of the vocabulary dimension, so that the i-th coordinate is 1 if the i-th word of the vocabulary is present in the sentence, and 0 otherwise. This implementation produces a computational and memory-efficient sparse matrix. For CountVect, we used word n-grams; specifically, only unigrams which yielded the best score. We ignored terms that appeared in more than 50% of the documents and in fewer than two documents.

Linear SVM

We choose a support vector machine with a linear kernel as algorithm used in this problem. SVMs are supervised machine learning models highly suitable for text classification problems. They only focus on the most difficult observations, whereas other classifiers pay attention to all data. The intuition behind the SVM approach is that if a classifier is good at the most challenging comparisons, then it will be even better at easier ones. The

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

two main advantages are a higher training speed and better performance with small and medium datasets, such as text datasets. We tried other algorithms as well, such as naive Bayes, random forest, and XGBoost, but the SVM yielded the best results. This was most noticeable for fake tweets in the test data, where SVMs were better by several percentage points relative to other algorithms. Figure 2 shows the classification report for the SVM on the train and test data. The F1 score was relevant because we had an unbalanced dataset.

	precision	recall	f1-score	support
0	0.93	0.83	0.88	4604
1	0.95	0.98	0.96	13952
accuracy			0.94	18556
macro avg	0.94	0.91	0.92	18556
weighted avg	0.94	0.94	0.94	18556

	precision	recall	f1-score	support
0	0.69	0.59	0.64	1151
1	0.87	0.91	0.89	3489
accuracy			0.83	4640
macro avg	0.78	0.75	0.77	4640
weighted avg	0.83	0.83	0.83	4640

Figure 2. SVM classification report.

The results are quite good and dis not assume that overfitting or underfitting had occurred. From the classification report, we can conclude that the model had more challenges in classifying fake tweets than real ones. This is reasonable, because fake tweets are a minority class, both in our dataset and in the real world, and are not easy to predict using their form. The SVM had several hyperparameters to be tuned. For kernels, we chose basic linear types, which are mainly preferred for text-classification problems because these are usually linearly separated with many features. In a later version, we could tune the SVM hyperparameters using Grid Search.

3.3.4. Testing

Results of The Performed Tests

For more accurate measurements, we used the F1 score; the F1 score formula is presented in Figure 3.

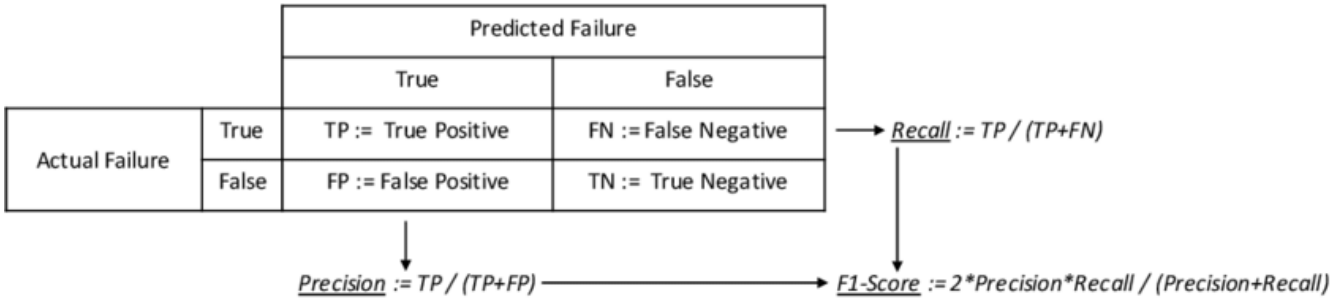

Figure 3. F1 score formula.

Using the F1 formula, we achieved the following F1 scores:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

- 88% for actual news;
- 64% for fake news.

The Use Case for Testing

To validate and evaluate the created solution, the testing focused on a practical use case that could be tested within a given timeframe and with an initial solution iteration. During the analysis of stablecoins, we identified the use case of Terraform Labs due to the significant data points in their social media announcements (Twitter) and other news sources (fake news analysis) reporting on the company due to the recent downfall of the value of their stablecoin. Given our objective research stance, we analyzed the Twitter account and news sources for the occurrence and evaluation of fake news.

The methodology of the testing will be as follows:

- Overall trustworthiness analysis of the company Twitter account;
- Overall trustworthiness analysis of the Company Founder's Twitter account;
- Analysis of the trustworthiness of the announcements and responses triggered by the news.

The testing showcased that, in the period before the crash, the OttCT algorithm had fewer triggers, but in May, there was a rise in the number of news alerts identified as untrustworthy (fake or nonfactual).

The company's Twitter account was evaluated with the OttCT model developed by Terraform Labs. The company was formed in 2018 to build the next Alipay, incorporated in Singapore but registered to operate its business as Terraform Labs in South Korea. The company was initially supported by four of the world's largest crypto exchanges at the time: Binance Labs, OKEx, Huobi Capital, and Dunamu (https://techcrunch.com/2018/08/29/terra/ accessed on 2 August 2022).

From the report by Chainalysis (a blockchain data platform providing data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries), "the downturn appears more closely linked to the tech market decline than to UST's collapse," but they also stated that "the UST's uncollateralized design likely made it more fragile than other Stablecoin types."

In addition to the subjective data and reasons that explain what caused the crash case, there was also the news about conspiracy theories and analysis of the historical situations that caused the crash.

Terraform official Twitter page and Terraform's Founder's Twitter page, in some cases, included personal announcements and comments on this news, as well as announcements of the launching of Terra 2.0 (Luna 2) as the new coin while referring to the former (close-to-no-value) LUNA coin as the Luna Classic.

The further developments of the situation, as well as the analysis of the critical events in the history of Terraform Labs that lost 99% of its value in 48 h, are part of the research on the ability of the OttCT to create the triggers for the protection of investments, resembling the case where Dolce & Gabbana lost 98% of their sales in China in a single day.

To tackle similar cases, additional testing and evaluations of the OttCT algorithm focus on other issues in the cryptocurrency market that we can conduct identical to the Terraform Labs.

Moreover, there are new cases in the cryptocurrency market. One of them is the case of the Celsius network, where the company froze (on 13.06.2022) an estimated USD 8 billion in deposits from its 1.7 million users. (https://www.washingtonpost.com/business/2022/06/13/celsius-crypto-bank-withdrawals-freeze/ accessed on 1 August 2022)

These events influence the cryptocurrency market at the time of the writing; therefore, establishing a triggering mechanism such as OttCT is of immense value for the overall protection of investors today and in the future. For this reason, we researched a use-case-specific business model that can use the initial iteration of the product already built as a protection tool for investors and investors' pools as possible initial users.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

3.3.5. Initial Test and Results

In the initial test of our working prototype, with the accuracy results presented above (88% for the factual news and 64% for the fake news), we conducted an experiment on the use case of the official Terraform Labs Company Twitter account.

For the conducted experiment, we took the time period of the week before the crash and the week following the crash, and found the following results:

- Week before the crash (1 May 2022 to 7 May 2022) (see Figure 4)

The result: 1 tweet out of 39 had OttCT grade 0 (0 may suggest a fake, nonfactual tweet).

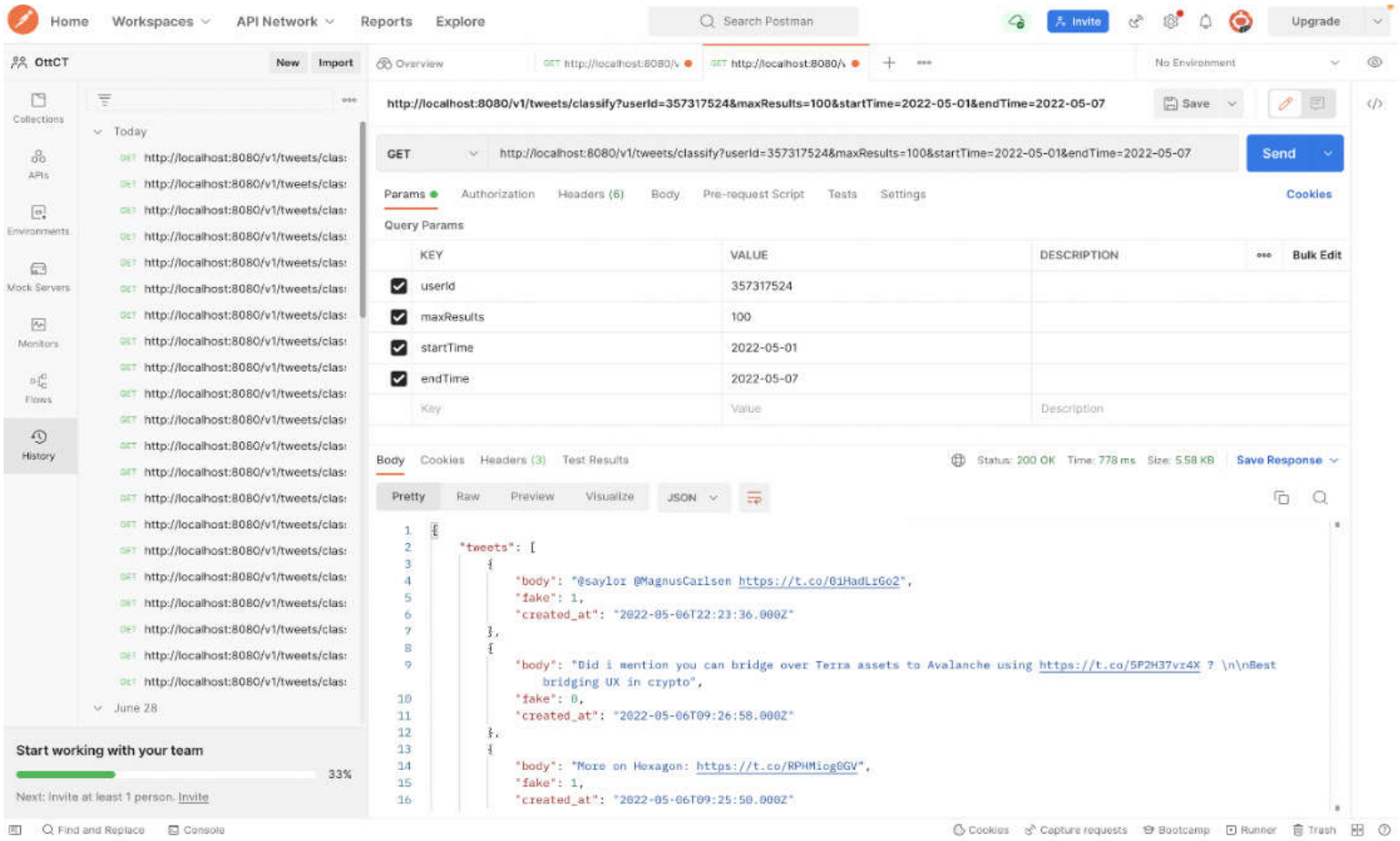

Figure 4. Results from the prototype on specific case 1.

- Week after the crash (7 May 2022 to 14 May 2022) (see Figure 5)

The result: 13 tweets out of 100 had OttCT grade 0 (0 may suggest a fake, nonfactual tweet).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

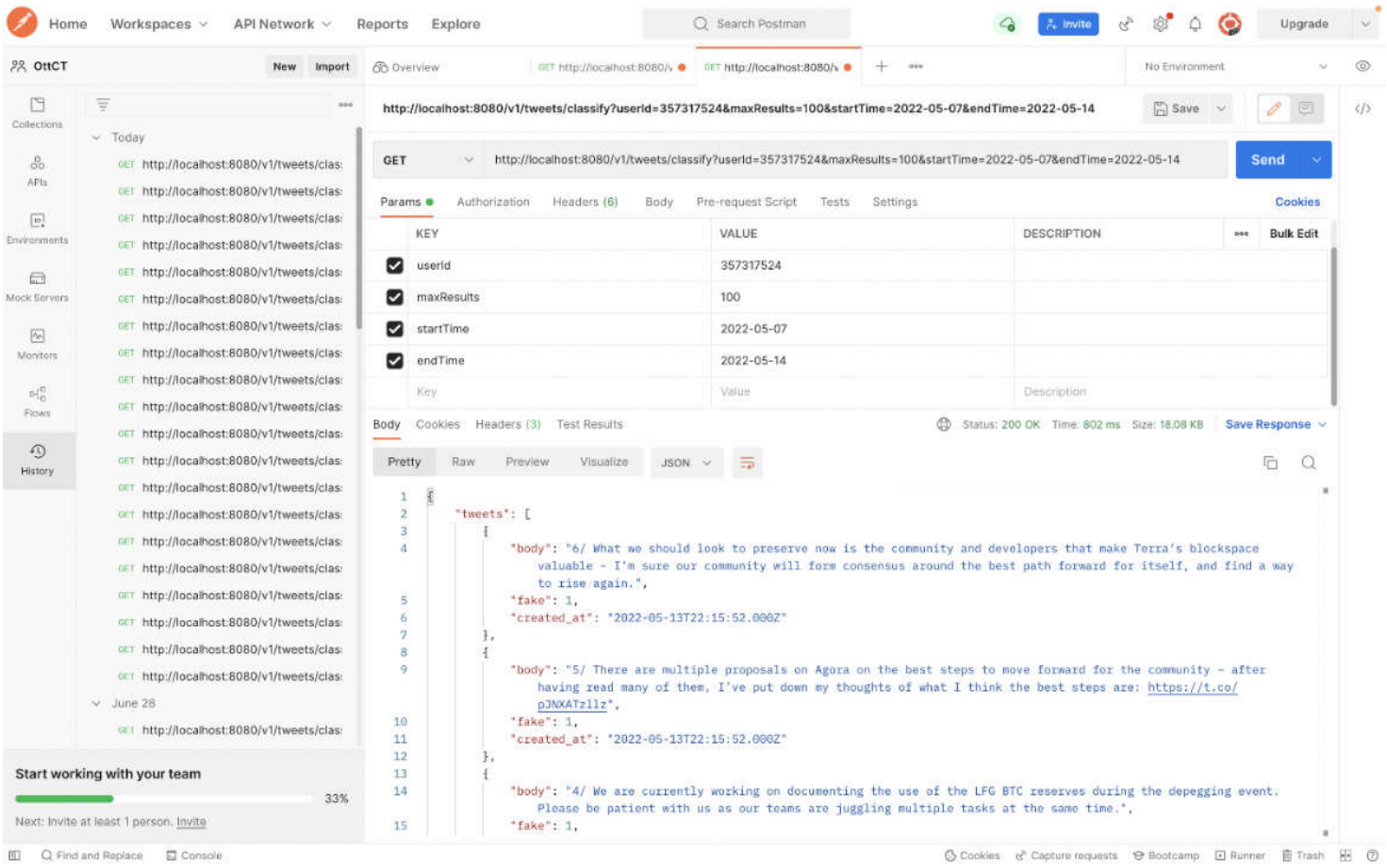

Figure 5. Results from the prototype on specific case 2.

The algorithm was improved and trained using a set news which was reported as fake (nonfactual and untrustworthy), including announcements and comments that did not resemble the truth. Due to the objective nature of the research, subsequent lawsuits in the Terraform case and examinations of the situation provided evidence of what was the truth as a final validation of the OttCT algorithm.

3.3.6. Evaluation

Evaluating the three metrics established in the Methodology (see above), the AI-led approach demonstrated a clear advantage towards manual information processing.

Cost as a metric refers to the monetary value of the measures from the perspective of the investor (user). More specifically, for social media tracking and debunking fake news, the metric is the cost for the adoption of the proposed protection framework compared with training a human to perform an equivalent task. Time as a metric refers to the time required for all steps of the procedure, from initiation to resolution, to be completed. The time measure more specifically operationalized here is the time taken for processing and reacting to the triggers (social media or economic). As mentioned above, the availability metric refers to the chances that the investor (user) will achieve a satisfactory outcome from the protection proceedings. In the context of the AI-led mechanism, it is a comparison of the accuracy of human- and computer-generated signals. Notably, in the business case, the triggering event simply allows a certain action to be taken by investors, should they deem it necessary. In that sense, we are developing symbiotic AI that would assist humans in making decisions. Consequently, the availability metric should focus on satisfactory—although highly probable—signals generated by the two evaluated approaches. Our prototype still has lots of testing and improvement to undergo; therefore, for the evaluation, we assumed that a trained human would do a better job than the AI.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

Table 3. Evaluation of technical characteristics.

	Current (Human)	OttCT (AI)
Time	Very slow	Very fast
Cost	Very high	Low
Availability	Very high	High

Table 3 indicates that the proposed protection framework is clearly superior to the current state of affairs, where manual labor is engaged with activities that are providing low added value.

3.4. Protections for Stablecoin Investors and Smart Contracts

Following the results of the research and taking into consideration the technical advances that can be incorporated in the protection framework, namely, smart contracts, we have developed an outline of the latter.

3.4.1. Actionable Protections

The actions that we envision investors to be able to perform (see Figure 6) could be classified in several key categories. We applied the above-mentioned methodology to assess the effects on possible liabilities for each category. The underlying assumption of this analysis is that we would like to avoid, as much as possible, any liability transfer and possible litigation complications. The summary below also indicates the specific legal tools to be employed to achieve the overall objective of reducing liability transfers.

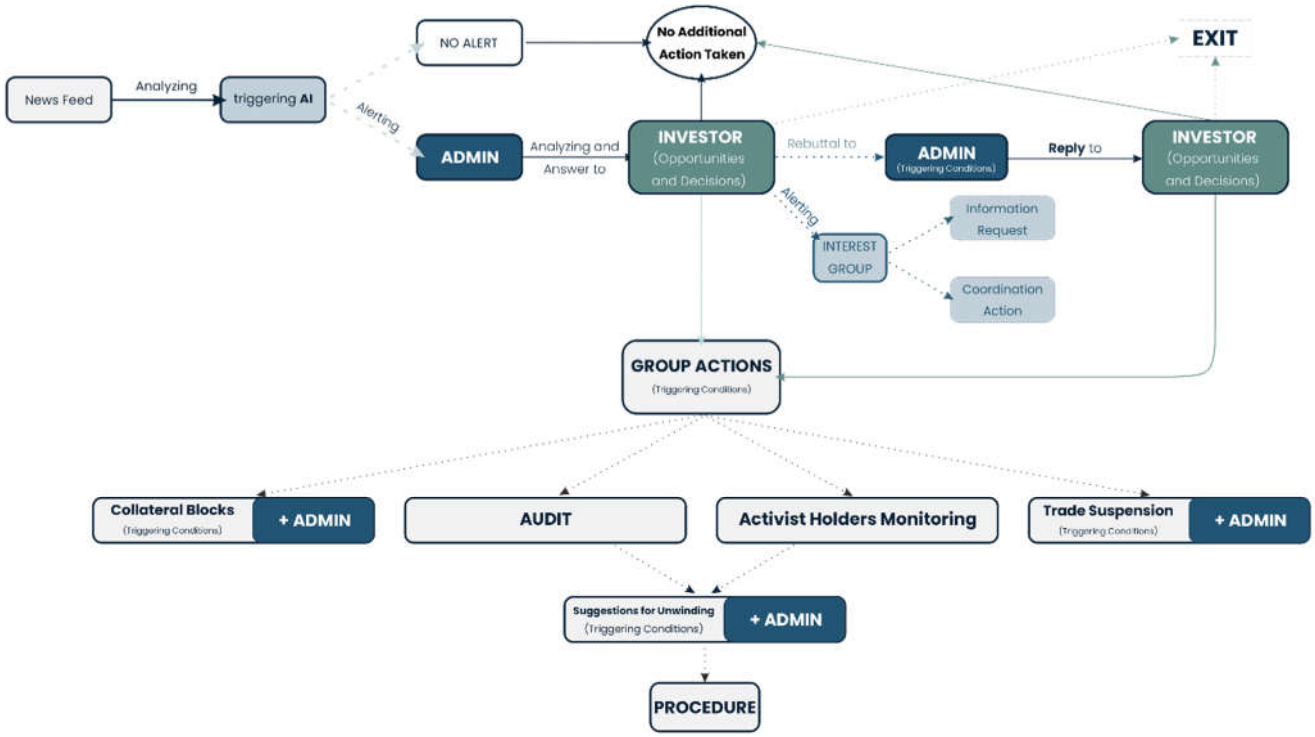

Figure 6. Actionable protections.

Action Category I: Information Inquiries

In this category, all the actions that provide investors or groups of investors with proactive information gathering are included. This not only covers the information provided directly by the administrator, but also indirectly through them by third parties (e.g., collateral custodians).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

Liability for the disclosure of sensitive information could be an issue for investors and their group actions, especially in the context of interest groups and public pressure campaigns. This could create a considerable tension and prolonged disputes regarding the leakage of confidential information. Therefore, we would suggest two specific approaches to mitigate the issue—blanket immunity to investors, and the creation of a single point of contact with the duty to safeguard any sensitive information.

Action Category II: Coordination Actions Concerning Altering the Discharge of Duties by the Administrator

These actions exclude weak protections, because the investors rely on the good will of a third party (e.g., regulators). The envisioned category of actions allows the administrator to decide whether the propositions are prudent or not at their own discretion. These group actions (see the graphics above) are the main actions we envision that stablecoin investors will enjoy.

There is a specific method of pressure in addition to the group actions—the entanglement of responsibilities. Fiduciary duty, which is the cornerstone of managerial responsibility, is the responsibility to act in the best interest of the company. The entanglement of responsibilities is a scenario where the coin holders (or an activist section of those) will provide clear indications as to what is the best interest of the company, whereas the manager should articulate why they would do otherwise. Should the proposition of the activists hold true, the manager may be personally liable for the poor decisions made. This will create a powerful tool to influence management on the key decisions for stablecoin.

The actions will still be made by the administrator; we do not anticipate specific issues on liability transfer.

Action Category III: Votes Binding on the Actions of the Administrator

The above category, in our suggestion, only covers actions relating to the dissolution of the stablecoin and asset liquidation. The votes are considered binding (as far as they do not infringe the bankruptcy law); therefore, the responsibility of the administrator will be shifted towards the voting (and non-voting) coin holders.

A number of legal tools (e.g., joint action concerning the implementation of trade suspension, cool-down period immunity from liability, actions by the investors envisioned in the collateral custodianship, etc.) would provide a considerable reduction in liability for activist coin holders in the third action category. However, liabilities may materialize, in certain circumstances. Therefore, in our proposed smart contract, we aimed to hardwire both the function to identify each vote, as well as liability limitation techniques that would provide sufficient legal revenues for those coin holders aiming to be activist and those of them satisfied as being in the majority. Those considerations will be taken in the development of the triggers and voting recommendations in the business design of our solution.

3.4.2. Smart Contract

The functionalities described above should be integrated into smart contracts together with bridges to oracles that would provide appropriate triggers. Those triggers would serve a dual purpose (see above), where they will: (a) provide alerts for investors, so they could decide what of the structured revenues for redress to follow; and (b) prevent abuse from third malicious actors, by acting as guards to the stablecoin administrator.

Specific issues for smart contracts involve the right for stablecoin investors to vote (e.g., collateral blocks). Those votes would need to reach certain thresholds to allow the corresponding action to be undertaken. In this article, we will not commit to specific recommendations concerning the votes, because these would vary depending on the business case of the stablecoin. However, the authors would urge any stablecoin design to take note of the results reached and discussed in this article.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0027.v1

3.4.3. Evaluation

Based on the Methodological notes (see above), the evaluation of the settled metrics for the protection of investor scores considerably better than the current situation. Concrete operationalization of the metrics would enable comparisons between the enforcement of smart contracts and the current protection enforcement exercised through the usual judicial channels.

Time in the general methodology refers to the time required for all steps of the procedure, from initiation to resolution, to be completed. For the comparison, it will be operationalized as the period required for stablecoin investors to receive a binding resolution concerning any grievance they may have against the stablecoin and its administrator. Cost as a metric refers to the monetary value of the said measures from the perspective of the investor (user). This is to be operationalized as the sum paid by the investor from the initiation of the complaint to the resolution. The availability metric refers to the chances that the investor will receive a satisfactory outcome from the protection proceedings, where a satisfactory outcome is defined as the recouping of all costs from a financially unfavorable event to the holdings of the investor in the stablecoin. Judicial proceedings take a very long time; therefore, the chances for law availability for the remedies, are extremely high (due to the high-speed nature of stablecoins).

Table 4. Evaluation of actionable protections.

	Current (Judicial)	OttCT (Smart Contract)
Time	Very slow	Very fast
Cost	Very high	Low
Availability	Low	High

In conclusion, we should note that protection through the integration of a smart contract is clearly far superior to the current situation.

4. Discussion

In this paper, we have demonstrated several key points that deserve deeper reflection, additional research, and discussion. Those points are furthering scientific understanding on the merger of several technological advancements in social context.

The first issue of discussion is the use of the metrics in this paper. We have took three aspects (time, cost, and availability) in their very abstract meanings and operationalized them for each of the technical aspects discussed here. Operationalization contextualized those three metrics in terms of the specific vertices of the examined subject (law, economics, or AI). However, there are possibly other metrics which we have not considered. Furthermore, the scale on which we performed the evaluation (very low–low–medium–high–very high) has relatively low granularity, and the boundaries between the categories are not very precise. However, in our view, this does not reduce the contributions of this paper in the slightest, although we realize that a valid discussion should be held on how best to measure the advantages a new protection framework for investors would bring.

Secondly, our paper has tackled a number of vertices to develop a more holistic and in-depth view of the protection framework. We explored dispute resolution, interest alignment for stakeholders, building trust through the utilization of AI, and the integration of all the above in an actionable framework for the protection of investors based on a DLT smart contract. However, the phenomenon we examined (investors' protection for stablecoins) is multifaceted, and additional dimensions might be relevant. In this regard, subsequent discussions concerning additions to the elements that are examined will be much welcomed.

Thirdly, a discussion we hope to encourage is the idea of the scalability of our proposed protections framework. Our innovation only started with stablecoins, but in the back of our mind we are considering CBDCs—notably, the Digital Euro. The parallels

 doi:10.20944/preprints202210.0027.v1

with stablecoins are remarkable. In that sense, we are looking at changing the entire paradigm of investing based on the CBDC infrastructure.

Finally, we hope to encourage discussions of our paper concerning actionable protection of the smart contract described herein. Those protections for stablecoin users are based on our original research, feedback from actual investors, and original analysis of existing revenues for stablecoin administrators and investors. However, we do not claim that the proposed actionable protections are unamendable. In contrast, we welcome any contributions and discussions for adding or changing any part of the actionable protections.

5. Conclusions

Our research was based on several testable propositions.

Proposition 1. *Stablecoin investors are not adequately protected.*

The collapse of Terra Luna was not insular occurrence in the field, as the loss of DEI's peg to the dollar demonstrated. These incidents were preceded by Empty set stablecoin, SafeCoin, BitUSD, DigitalDollar, and NuBits. Investors in all those projects were not adequately protected. Tera Luna's sheer size made it headline news, but the underlying problem remains.

Proposition 2. *DLT provides a new set of protection options.*

A list of protection measures is included in this paper that could only work in the setting of a crypto space. The advantages for using such protections are numerous and thoroughly described above. We argue that those protections would make a difference. The simulation we have created for advanced alert signaling (see Section 3.3), together with the advanced options for collateral blocks, cool-down periods, and extended reviews of trustworthy information (both gathering and communication) described above (see Section 3.4), provides very strong bases for our claim that OttCT would have made a difference for investors. It is debatable whether utilizing our protection measures would have safeguarded 100% of the investment, or 80% of it. What is certain, however, is that the loss of investors would have been much smaller than their total exodus in the current situation. As such, we contest, with a high degree of certainty, that DLT provides a new set of protection options that should be utilized for the sake of both investors and stablecoins.

Proposition 3. *The protection options can be operationalized in a working prototype of actionable protections.*

Thanks to the generous support of the European Commission under the TruBlo Program, with the help of our esteemed co-workers Milica Sokolovic, Asparuh Kebonin, and Iliya Vassilev, we have created a working prototype of the proposed protection framework. More information can be found by visiting the website at www.ottct.com.

Proposition 4. *Protection frameworks for investors in stablecoins can be duplicated for investors in various investors' trust, crowd-funded, and security-based common investment schemes, when CBDCs are expected to be more widely adopted towards the middle of this decade.*

The stablecoins business model provides access to funding for various innovative business entities and connect them with investors and/or lenders. The central feature of a stablecoin is its peg to underlying currency (e.g., Euro). If we were to subsidize the upcoming Digital Euro with stablecoins, the very same obstacles, trust issues, and susceptibility to fake news would remain for all sorts of investment schemes (ETFs, real estate trusts, impact investment vehicles, etc.) The Digital Euro represents a chance to upgrade

 doi:10.20944/preprints202210.0027.v1

protections for all Europeans, and work towards a more equitable investment climate, while at the same time increasing transparency, trust, and security for both professional and retail investors.

We consider that the arguments we have provided to support our propositions are compelling. As such, we could conclude that there is a need for workable solutions for investors in stablecoins. Moreover, we have demonstrated that these workable solutions are feasible.

As far as a unique contribution to contemporary scientific knowledge, this article presents an innovative and internally coherent view on integrating a host of protections and procedures for stablecoin investors in a holistic product. Utilizing DLT and AI, creating the financial incentives for stakeholders to participate, and bringing together on-chain and off-chain actions is a uniquely positioned result.

We began this article with the collapse of Terra Luna, and we finish it with a pathway towards preventing this from happening in the future. Based on our research, we can confidently claim that such a path is possible, plausible, and achievable.

Author Contributions: Conceptualization, Dimitar Kyosev and Orfefs Voutyras.; methodology, Dimitar Kyosev; software, Dimitar Anastasovski.; validation, Dimitar Anastasovski, and Mirko Kikovic.; formal analysis, Dimitar Anastasovski; investigation, Dimitar Kyosev, Dimitar Anastasovski, Mirko Kikovic and Orfefs Voutyras; resources, Mirko Kikovic and Orfefs Voutyras; data curation, Dimitar Anastasovski; writing—original draft preparation, Dimitar Kyosev.; writing—review and editing, Dimitar Kyosev; supervision, Orfefs Voutyras.; project administration, Mirko Kikovic.; funding acquisition, Mirko Kikovic. All authors have read and agreed to the published version of the manuscript.

Funding: Next Generation Internet TruBlo Program for enhancing trust through the use of DLT. The APC was funded under Grant Agreement 957228 of H2020.

Informed Consent Statement: Not applicable

Data Availability Statement: During the study we have analyzed public records on the Tweeter (https://twitter.com/terra_money?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor) social media.

Acknowledgments: This paper has been produced with the financial support of the European Commission, under the NGI TruBlo Program for enhancing trust through the use of DLT.

Conflicts of Interest: The authors declare no conflict of interest

References

1. Chohan, U.W. Are Stable Coins Stable? (29 March 2020). Notes on the 21st Century (CBRi), 2019. Available online: https://ssrn.com/abstract=3326823 (accessed on 29 July 2022).
2. Doerr, J.F.; Kosse, A.; Khan, A.; Lewrick, U.; Mojon, B.; Nolens, B.; Rice, T. DeFi risks and the decentralisation illusion. *BIS Q. Rev. December* **2021**, 21.
3. Picard, F. Decentralized finance and investor's protection: How this alternative financial system may have a place in Europe 2021; Available online: https://www.researchgate.net/publication/358575212_Decentralized_finance_and_investor%27s_protection_KYC_how_this_alternative_financial_system_may_have_a_place_in_Europe_-_Master%27s_thesis_-_Financial_risk_management (accessed on 17 July 2022).
4. Dhar, T. Stablecoins Ecosystem: A Promise That Can Be Kept (25 January 2020). Available online: https://ssrn.com/abstract=3581876 (accessed on 1 August 2022).
5. Cao, Y.; Dai, M.; Kou, S.; Li, L.; Yang, C. Designing Stable Coins. 2021. Available online: https://ssrn.com/abstract=3856569 (accessed on 30 July 2022).
6. Wang, G.J.; Ma, X.Y.; Wu, H.Y. Are stablecoins truly diversifiers, hedges, or safe havens against traditional cryptocurrencies as their name suggests? *Res. Int. Bus. Financ.* **2020**, *54*, 101225.
7. Baur, D.; Hoang, L. A crypto safe haven against Bitcoin. *Financ. Res. Lett.* **2021**, *38*, 101431; DOI: 10.1016/j.frl.2020.101431

8. Arner, D.W.; Auer, R.; Frost, J. Stablecoins: Risks, Potential and Regulation. 2020. Available online: https://ssrn.com/abstract=3979495 (accessed on 1 August 2022).
9. Kampakis, S. Auditing Tokenomics: A Case Study and Lessons from Auditing a Stablecoin Project. *J. Br. Blockchain Assoc.* **2022**, 34696.
10. Choi, G. TOK Stablecoin: A Catalyst for DeFi Ecosystem Expansion. 2022. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4123399 (accessed on 3 August 2022).
11. Nøkleholm, B.A.; Kviseth, G.V. Regulation of Cryptocurrency: An Analysis of the Proposed Markets in Crypto-Assets Regulation Emphasizing on the Issuer of Stablecoin. Master's Thesis, Handelshøyskolen BI, Oslo, Norway, 2021.
12. Hemenway Falk, B.; Hammer, S. Meltdown in the Wild West: The Stablecoin Collapse of 2022 and Consumer Protection Considerations. 2022. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119627 (accessed on 1 August 2022).
13. Uhlig, H. *A Luna-tic Stablecoin Crash*; (No. w30256); National Bureau of Economic Research: Cambridge, MA, USA, 2022. Available online: https://www.nber.org/system/files/working_papers/w30256/w30256.pdf (accessed on 2 August 2022)
14. Greenlaw, S.; Shapiro, D. Principles of Macroeconomics, Open Textbook Library. 2017. Available online: https://open.umn.edu/opentextbooks/textbooks/192 (accessed on 1 April 2022)
15. Reinert, E. How Rich Countries Got Rich and Why Poor Countries Stay Poor; Constable & Robinson: London, UK, 2007.
16. Auer, R.; Böhme, R. The Technology of Retail Central Bank Digital Currency. BIS Quarterly Review, March 2020. Available online: https://ssrn.com/abstract=3561198 (accessed on 7 July 2022).
17. Gugler, K.; Mueller, D.C.; Yurtoglu, B.B. Corporate governance and globalization. *Oxf. Rev. Econ. Policy* **2004**, *20*, 129–156.
18. Asril, J. Legal Protection for The Minority Shareholders as The Implication of National Company Stock Acquisition by Foreign Company Within The Globalization Era. In Proceedings of the International Joint Seminar, Macao, China, 10–16 August 2019; p. 159.
19. Mokhtarian, E.; Lindgren, A. Rise of the Crypto Hedge Fund: Operational Issues and Best Practices for an Emergent Investment Industry. *Stan. JL Bus. Fin.* **2018**, *23*, 112.
20. Snow, N.M. Retail Investors' Perceptions of Financial Disclosures on Social Media: An Experimental Investigation Using Twitter. 2015. Available online: https://digitalcommons.usf.edu/etd/5880/ (accessed on 11 June 2022)
21. Mikołajewicz-Woźniak, A.; Scheibe, A. Social media in company's communication with investors. *Handel Wewnętrzny* **2017**, *2*, 270–279.
22. Black, B. Behavioral economics and investor protection: Reasonable investors, efficient markets. *Loy. U. Chi. LJ* **2012**, *44*, 1493.
23. Costola, M.; Iacopini, M.; Santagiustina, C. On the" mementum" of Meme Stocks. *arXiv* **2021**, arXiv:2106.03691.
24. O'Connor, T.; Kinsella, S.; O'Sullivan, V. Legal protection of investors, corporate governance, and investable premia in emerging markets. *Int. Rev. Econ. Financ.* **2014**, *29*, 426–439.
25. Zhu, H.; Zhou, Z.Z. Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. *Financ. Innov.* **2016**, *2*, 1–11.
26. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express* **2021**, *7*, 229–233.
27. Shi, E. Foundations on Distributed Consensus and Blockchains (book draft). 2021.Available online: https://www.distributedconsensus.net/ (accessed on 12 June 2022)
28. Kuo, T.T.; Zavaleta Rojas, H.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478.
29. Babbie, E. The Practice of Social Research. Thomson Wadsworth. Belmont, CA. 2007. ISBN-10: 0-495-18738-0
30. Giannetti, M.; Koskinen, Y. Investor Protection, Equity Returns, and Financial Globalization. *J. Financ. Quant. Anal.* **2010**, *45*, 135–168. Available online: http://www.jstor.org/stable/27801477 (accessed on 15 May 2022).