PrimeRating

Fundamental Report

Prime Rating Report V2.1

Protocol: Tornado Cash
Version:
Date: 07/04/2022
Previous Report: Link to previous report

Author: Salomé
Reviewed by: xm3van
Season/competition:

Scorecard

1. Value Proposition	Points
a) Novelty of the solution	12 / 15
b) Market fit/demand	11 / 15
c) Target Market Size	10 / 10
d) Competitiveness within market sector(s)	10 / 10
e) Integrations & Partnerships	2 / 15
Total Points - Value Proposition	**45 / 65**
2. Tokeneconomics	**Points**
a) Is the token sufficiently distributed?	14 / 15
b) What is the extent of the token's capabilities?	6 / 10
c) Is the issuance model able to improve the coordination of the protocol?	8 / 10
d) Is the value capture model able to accrue and distribute value?	8 / 10
e) Is the token sufficiently liquid to enable active use and trade?	5 / 5
f) Are there any extrinsic productivity use cases?	5 / 10
Total Points - Tokenomics	**46 / 60**
3. Team	**Points**
a) Is the team credible and public? (No, Partly, Yes & Anon , Yes & Public)	15 / 15
b) Does the team have relevant experience?	10 / 10
c) Does the team participate and help shape the public debate?	4 / 5
d) Is the team able to effectively attract and coordinate resources?	8 / 10
Total Points - Team	**37 / 40**
4. Governance	**Points**

a) Admin Keys	**20 / 20**
b) Extent of Governance capabilities	**15 / 15**
c) Active Governance contributors	**3 / 5**
d) Governance infrastructure	**10 /10**
e) Robustness of Governance process	**10 / 10**
Total Points - Governance	**58 / 60**
5. Regulatory	**Points**
a) Does the protocol have any legal accountability?	**n/a / 15**
b) What is the quality of the legal jurisdiction?	**n/a / 10**
Total Points - Regulatory	**n/a / 25**
Total	**186 / 225**

1. Value Proposition

The Value Proposition section describes the value a protocol delivers to its users. Based on the proportion of the problem the protocol aims to solve and the potential of the protocol to effectively solve the problem - better than other industry solutions - a Value Proposition rating is created.

a) Novelty of the solution (15 points)

This score evaluates the novelty (uniqueness) of the protocol. Has the protocol introduced any new innovations that help solve user's problems more efficiently? Is the project a fork? To what extent did they copy/fork the original?

Answer: Tornado Cash is a fully decentralised non-custodial protocol allowing private transactions in the crypto-space. Tornado.Cash smart contracts have been implemented within the Ethereum blockchain, making them immutable. They can neither be changed nor tampered, therefore, nobody - including the original developers - can modify or shut them down. Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. The Tornado Cash protocol was developed based on open source research by the Zcash team in collaboration with the Ethereum community.

Since its initial launch in 2019, the protocol has been offering diversified fixed amount pools for six tokens (ETH, DAI, cDAI, USDC, USDT, and WBTC). As of June 2021, in addition to the Ethereum blockchain, Tornado Cash smart contracts have also been deployed on other side-chains & blockchains. These deployments enabled the tool to either support new tokens or benefit from Layer-2 advantages, such as faster and cheaper transactions. See details here.

Tornado Cash is currently operating on:

- Ethereum Blockchain : (ETH, DAI, cDAI, USDC, USDT, and WBTC)
- Binance Smart Chain: (BNB)
- Polygon Network: (MATIC)
- Gnosis Chain: (xDai)
- Avalanche Mainnet: (AVAX)
- Optimism: (ETH)

- Arbitrum One, as a Layer-2 (ETH)

In December 2021 a upgraded pool Tornado Cash Nova has been added to the protocol (still in beta). Users are no longer restricted to fixed-amount transactions. Users can take advantage of an arbitrary amount pool and shielded transfers. In order to optimise speed and cost, Tornado Cash Nova operates on the Gnosis Chain (formerly xDai Chain). ETH amounts can be deposited or withdrawn in any quantity. Besides shielded transactions, this pool also allows users to transfer custody of their tokens while remaining in the pool.

Users can also prove the link between a deposit and a withdrawal with Tornado Cash's compliance tool. It gives the user the freedom to disclose the information if needed. There is no requirement that financial information is completely hidden, and the user has the power to decide who can see it. Crypto mixing services haven been used already for a while and are not a complete novel idea (example Bitcoin Fog).

Organisational innovation has been proven by Tornado Cash as the protocol is completely decentralized, controlled and governed by its community on-chain. Also the Community Fund to compensate contributors has shown to be a key role in the growth of Tornado Cash.

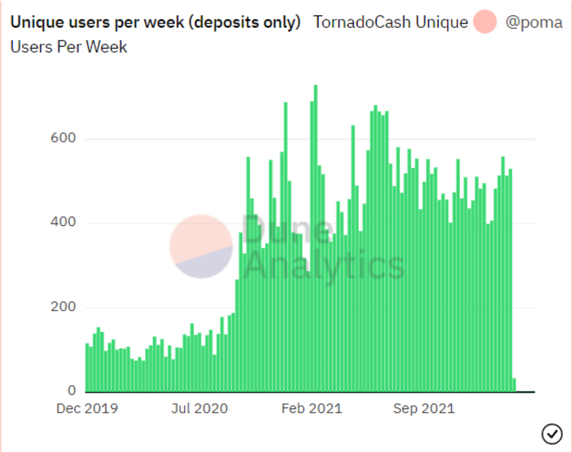
Score: 12

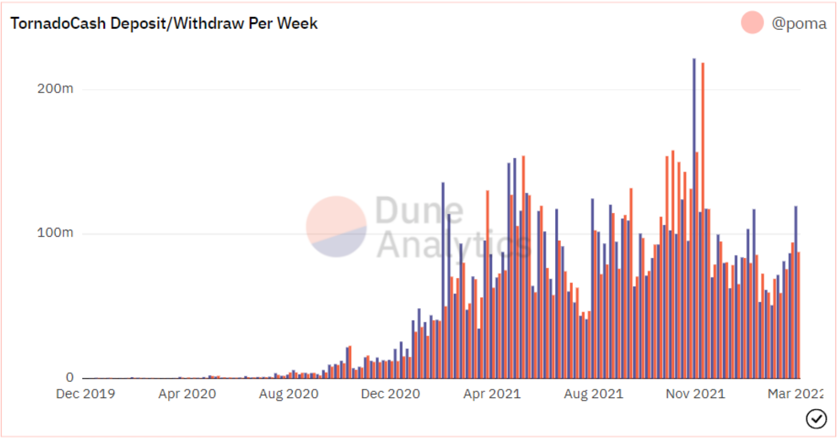
b) Market fit/demand (15 points)

This score evaluates the degree to which the protocol satisfies a strong market demand. The market fit evaluates if the protocol is able to satisfy the needs of a specific market (can also be measured by user adoption/ #of users). To what extent has the protocol proven to meet the demand of a specific market? Is the timing of the product right for the market? Is the protocol targeting the right market?

Answer: To assess the market fit, it is necessary to dispel the myth that cryptocurrency transactions are private. The on-chain privacy of public blockchains like Ethereum is essentially nonexistent, since anyone can inspect the public ledger to learn about every wallet's transaction history. It's essential to have ways to protect information and keep sensitive data safe. Tornado Cash is a valuable weapon in the battle for privacy and security while still reaping the benefits of a decentralised blockchain network. As Tornado Cash does not only operate on L1 but several other blockchains, as stated above, the market is tremendously. Tornado Cash has achieved a clear market by facilitating 2,765,644 ETH (currently ~$6,151,707,161) worth of transactions across 45,020 unique users. Meaning that Tornado Cashs facilitated around 2.29% of Etheriums total current circulation supply of 120,299,297 ETH.

By looking at the historical withdrawals/deposits stats per week it is visible that there is a growing interest of users seeking privacy, so far the protocol has shown clear signs of a market fit in a promising market.





Source https://dune.xyz/poma/tornado-cash_1

Score: 11

c) Target market size? (10 points)

The target market size evaluates the current and future size of the problem the protocol is aiming to solve. The category of the Open Finance solution can be used as a reference to the target market (for example: Lending). Because Open Finance is by definition global, the global market for a specific problem equals the target market size.

Answer: Although we can anticipate a multi-chain universe in the future with many chains for various use cases, it is still difficult to assign a concrete market size to the demand for private transactions. In any case, this market is likely to be huge, and the best analogy is assuming that users will seek privacy even more once regulatory policies catch up with crypto. As the concrete market size can not be established the potential is infinite. If it is assumed that crypto users are strong believers of privacy, protocols and applications like Tornado Cash will have exponential growth in the near future.

Score: 10

d) Competitiveness within market sector(s) (10 points)

This score evaluates the competitiveness of the protocol within the market sector(s) it operates in. This score offers a relative comparison of the protocol and other protocols operating in the same market sector(s). To evaluate this, metrics to directly compare with the competition can be used (e.g. TVL, trading volume, number of users).

Answer:

Tornado Cash is the largest private transaction middleware on Ethereum. Tornado Cash has been developed using open-source code from Zcash.

Zcash and Monero for example are standalone privacy coins, whereas Tornado Cash is a coin-agnostic anonymity mixer, which makes it more popular.

A standalone privacy coin's default privacy makes auditing more difficult; for instance, a bug could cause the Monero money supply to increase in an unnoticeable way. (Inflation bugs have also been observed in public blockchain cryptocurrencies like Bitcoin and hybrid cryptocurrencies like Zcash). This problem is also acknowledged by Monero developers, shielded Zcash transactions present a similar audibility problem.

Typhoon Cash, Typhoon Network, and Cyclone can all be seen as direct competitors. Compared to Tornado Cash, however, none of the above-mentioned projects has yet demonstrated any benefits and increased financial support. To conclude, Tornado Cash has no strong and original coin-agnostic anonymity mixer competitors at the moment and is the benchmark of the market segment.

Score: 10

e) Integrations & Partnerships (15 points)

Due to crypto's open-source nature, the code of most protocols can easily be forked. This score represents a piece of "unforkable value". Some indicators to look at are the number of applications built on top of the protocol (vertical integration), other entities integrating the protocol's services (horizontal integration) or the number of relevant partnerships (be careful of logo collections/ partnerships without much purpose).

Answer: Although the dapp can be used for integrations and partnerships because it has the purpose of allowing anonymous interactions but as of today the DAO doesn't seem to focus on pursuing any.

Score: 2

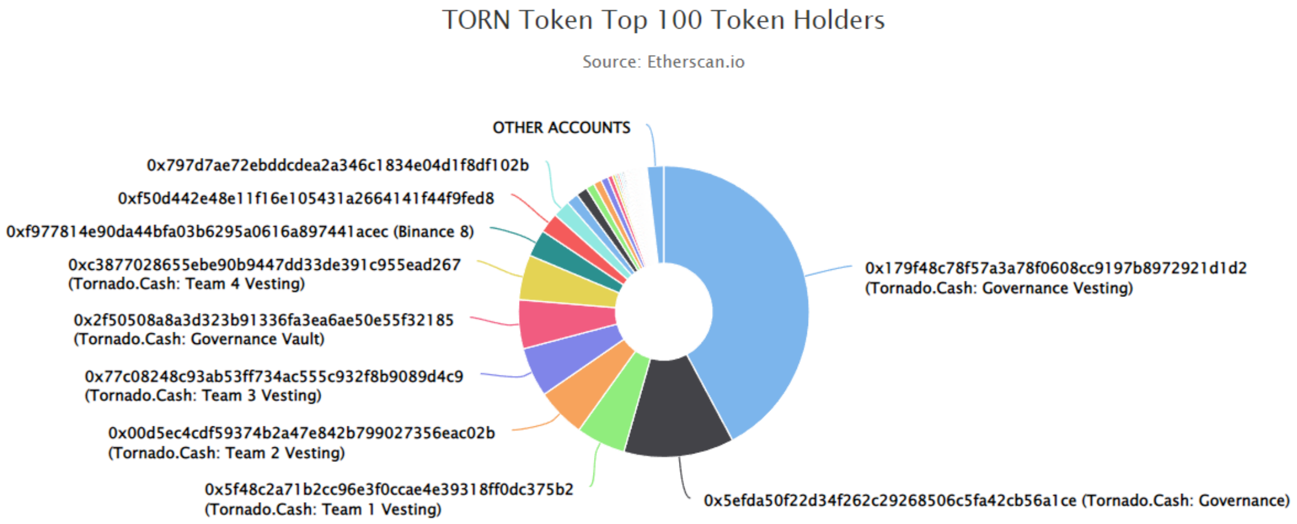
2. Tokeneconomics

The Tokeneonomics section assesses the function of a protocol's token. This includes the token distribution, functionalities of the token, the ability of the token to incentivize positive behaviour in the protocol, and the ability of the token to capture a portion of the value created.

a) Is the token sufficiently distributed? (15 points)

The token distribution can be an indicator of a healthy protocol. When the protocol tokens are widely distributed among different stakeholder groups and contributors, this genuinely improves the coordinating capability of the token and strengthens the resiliency of the protocol. Was the initial distribution balanced between relevant stakeholders? Are the tokens distributed over sufficient participants (10, 25, 100 largest addresses)?

Answer: $TORNI has a total of 7,744 token holders at the time of writing. The current token supply is distributed towards many token holders. There is no disproportionate distribution towards a small group of users see here.


TORN Token Top 100 Token Holders

Source: Etherscan.io

So far, Tornado Cash facilitated 2,709,817 ETH worth of transactions across 45,020 users. It seems that the token is distributed effectively in a decentralized way and improves the protocol efficiency in collaboration with token holders. Tornado Cash did an airdrop in Feb. 2021 with 5% (500,000 TORN tokens) of its total supply of 10 million. TORN tokens are 55% owned by the community and treasury (5,5 million TORN), gradually unlocking over a five-year period. While developers and investors maintain a 30% (3 million TORN) stake in TORN’s total supply, see more details about the TORN tokenomics here.

Score: 14

b) What is the extent of the token's capabilities? (10 points)

Is the token useful within the protocol? Does the token allow the holders to participate in governance or influence the protocol in any way? Does it serve any other purposes?

Answer: Tornado Cash uses $TORN tokens for governance and revenue. The token is currently used for Governance, LP staking (extrinsic use case), staking & being a Relayer of the Tornado Cash Ecosystem (the only condition to be included on the Tornado Cash UI is to hold a min. of 300 TORN). Tornado Cash's relayers are a vital component of its ecosystem. Due to their use, they guarantee privacy when withdrawing tokens from a pool as they solve the dilemma of how to pay withdrawal fees while staying anonymous.

Score: 6

c) Is the issuance/distribution model able to improve the coordination of the protocol? (10 points)

To what extent does the issuance of the token support the advancement and function of the protocol? Are the tokens justifiably being issued? Does the issuance model incentivize the right behaviour? Are all relevant stakeholders benefiting from the issuance model?

Answer:

Yes, the token issuance model is incentivising the right behaviour and improving the protocol. The Tornado.Cash distribution plan issued a fixed total of 10 million TORN governance tokens, all of which will be circulated in five years. An initial 5% of the total governance tokens were airdropped to the users, and 10% will be distributed through a mechanism called " Anonymity Mining ". Through anonymity mining, users can participate in liquidity mining while keeping their anonymity. The model takes into account the speed of token distribution and market fluctuations. To enhance the privacy of the entire process, Tornado.Cash developed a two-layer token model. Participation in anonymous mining activities does not directly result in TORN, but rather an intermediate asset called "Anonymity Points". On the chain, this part of the asset will not be recorded as a direct amount. Instead, it will be calculated through zero-knowledge proof. Along with 5% airdrops, 10% mining, 30% allocated to the team and investors, 55% will be allocated to the management of the DAO's treasury, which will unlock linearly over five years.

The community also proposed a Community Fund (proposal #7) to allocate 5% of the total available TORN of the governance treasury, to reward contributors.

Score: 8

d) Is the value capture model able to accrue and distribute value? (10 points)

A value accrual and distribution mechanism can help improve the utility of a token and its ability to be used as an effective coordination mechanism. Does the protocol have mechanisms to distribute some of the value created to the token holders?

Answer: Yes through $TORN staking, LPing and the relayer system. When a relayer is used in the Tornado Cash pool, a small amount of TORN is automatically collected from this staked balance by the StakingReward contract. Maintaining a stakes balance of minimum 300 TORN at all times is a key element, as relayers are required to do so (governance can change the minimum stake). A portion of the collected fees is then distributed among DAO members with lockedTORN tokens. TORN are also required to be locked to participate in on-chain and off-chain governance (submitting & voting on proposals). So all token holders which are staking TORN are able to receive a portion of the fees collected by the protocol from relayers.

Score: 8

e) Is the token sufficiently liquid to enable active use and trade? (5 points)

Is the token widely available and is there sufficient liquidity available to facilitate all protocol functionalities?

Answer: The token is available on most DEXs and CEXs and has deep liquidity, see all markets here. Their overall 24h trading volume is around ~$43,7M. The Coinmarketcap liquidity scoring system indicated a liquid market.

Score: 5

f) Are there any extrinsic productivity use cases for the token? (10 points)

Besides the protocol's value distribution model as described in 2. d), can the token be used productively on other protocols (e.g. as collateral, for lending, LPing, yield farming, etc.)?

Answer: As stated in 2. d) the token can be used in other protocols for LPing and staking. Apart from that there are no other use cases for the token. Tornado Cash however is supported on several Blockchains such as Ethereum Mainnet, Binance Smart Chain, Polygon Network, Optimism, Arbitrum One, Gnosis Chain, Avalanche Mainnet and Ethereum Goerli.

Score: 5

3. Team

The Team section describes the quality of the team behind the protocol. The current version of Prime Rating favours teams that are publicly identifiable. In the case of an anon team, the track record of the specific anons involved can be taken into account

a) Is the team credible and public? (15 points)

Are the identities of the core contributors and team publicly identified? In the case of anon team members, is there any way to track their background/record?

Answer: Yes the founder identities are public and of some of the team members (see forum, snapshot votes to reward contributors). The protocol was developed by withheld hackers from Peppersec. The known creators of the protocol are Roman Semenov (Twitter / Linkedin) and Roman Storm (Twitter / Linkedin). See more about their backgrounds in 3. b). Tornado Cash protocol is developed based on open source research in collaboration with the Zcash team and talents from the Ethereum community.

Score: 15

b) Does the team have relevant experience? (10 points)

Are there any documents or trails available to showcase the track record of the team? Do the team members have relevant backgrounds and skill sets?

Answer: Both founders have a highly credible background with impressive experience. While Storm is formally educated in Metallurgical Engineering, he has been intrigued by blockchain technology since 2011. His previous experience includes Blockchainlabs.nz, Amazon, PepperSec, and DeFi projects such as 0x, Aave, Compound, MakerDAO, and 1inch. He audited Solidity code, created smart contracts and created ERC-20 tokens across these companies/protocols. The education of Roman Semenov is equally impressive, specialising in fields such as field theory and quantum statistics. As the founder of PepperSec and Viking Studio, a Russian social media marketing firm, he has honed his skills at RedHelper, which optimizes e-commerce funnels and conversions. The Tornado cash team & community have proven themselves by the technical innovations they have implemented and it shows that they have all the skills to deliver the project as a whole.

Score: 10

c) Does the team participate and help shape the public debate? (5 points)

To what extent do the protocol contributors participate in the public debate around open finance? Are the team members giving presentations, sharing their thoughts and opinions, and do they help raise the collective intelligence of the industry?

Answer: The founders are public figures participating in podcasts, talks, keynotes and public media see some examples here, here, here, here. Tornado Cash is often mentioned in news related to illegal and privacy focused activities. Also the founders are active on Twitter and other social media platforms such as blogs and regularly share their opinions online. The activity of the founders in the Tornado Cash Governace forum has decreased since the last year, however the project is managed actively by its community and contributors. The founders are shaping the crypto space by contributing to several open source projects.

Score: 4

d) Is the team able to effectively attract and coordinate resources? (10 points)

How effective is the team at attracting and coordinating resources for the benefit of the protocol? Has the team raised sufficient funding or are there mechanisms in place to attract resources when needed?

Answer: The team has attracted a lot of attention from the crypto ecosystem and has been able to attract resources. Given the fact that the Tornado Cash team decided to do a fair launch (airdrop) without being capital hungry, it shows that the team can coordinate efficiently, see more details here. Moreover, Tornado Cash has a Community fund to reward contributions and therefore attract new talents to the protocol. The community allocated 5% of total available TORN tokens of the governance treasury to the Community fund (approximately 78k TORN). Since the protocol launch Tornado Cash has collected a total amount of $11,26M in fees and managed to cover all expenses with protocol revenues.

Score: 8

4. Governance

The Governance section evaluates how the protocol is governed and who the governors are. The different governance functionalities and processes are evaluated to determine to what extent the Protocol will be able to self-govern in a way that ensures the development of the protocols while respecting the needs of all current and future stakeholders.

a) Admin Keys (20 points)

Admin Keys allow some critical functionalities of a protocol to be controlled by an admin. This allows the developers to react to potential bugs, but also creates a risk as the developers could potentially misuse the admin keys to exploit the protocol. Does the protocol have admin keys and how are they managed?

Answer: The protocol is permissionless code since 10 May 2021 as the Developers of Tornado Cash have destroyed their admin keys. Since then the protocol is completely trustless without any admins and no upgradability possibility. Nobody, including the Tornado Cash developers, has the ability to alter the protocol or shut it down. The UI is hosted on IPFS by the community, as long as at least one user hosts it, it is accessible.

Score: 20

b) Extent of Governance capabilities (15 points)

Distributed governance allows the token holders to participate in the governance of open finance protocols. How much influence does the governance mechanism have? Are the votes affecting on-chain changes or do they function solely as signals to the team?

Answer: Governance influences all operations of the protocol including on-chain changes, protocol parameters and token distribution. All Tornado Cash smart contracts, including those for governance and mining, are decentralised. See more details about Tornados Governance here.

Score: 15

c) Active Governance contributors (5 points)

Governance is a process that can be rather resource-intensive if executed well. To ensure good governance is practiced by the protocol, it's important to have a sufficient number of governors allocate resources to the governance process of the protocol. How many individuals participate in the debate around the protocol? How active are voters?

Answer: Community contributors participate actively in the Governance forum and shape the debates in Discord & Telegram. There are currently 1,177 Governance Voters and the community voters seems still growing.

Looking at the last on-chain votes here, the number of tokens participating has an average of around 24k. With a circulating supply of around $1,75M TORN tokens, that's an average of ~1.36% participation rate. For more details about their on-chain Governance stats see the Dune Dashboard here.

Tornado.Cash also has a Community Fund , to award its key contributors. It was implemented by the community in June 2021 see proposal #7. The Snapshot votes who decide on community contributors compensation have an average of 13 voters per proposal which is rather low.

Key stats for Tornado Cash's social media platforms as of report date:

Telegram: ~5281 members
Twitter: ~42.4K followers

Discord: ~1047 members
Forum: ~1152 users

Tornado Cash seems to have a diverse group of active governors who contribute and participate in the debate to shape the protocol, however there is potential to grow the community and participation.

Score: 3

d) Governance technology/infrastructure (10 points)

The Governance infrastructure relates to the technology, software, and models used by the protocol's governance. Does the protocol have a reliable and usable voting mechanism? Are there channels for governance debate? Is there sufficient documentation available?

Answer: The protocol has a reliable decentralised and useful governance infrastructure which is documented here. Governance discussions take place in the Tornado Cash forum, Discord and Telegram. The governance infrastructure allows the community to shape, improve the protocol, participate in suggesting proposals and expressing their opinion through votes. See more about the community involvement here. All proposals go through an on-chain voting process, see all proposals here.

Score: 10

e) Robustness of Governance process (10 points)

This score requires documentation specifically on the governance process that sets the basic framework in terms of agreements, norms, and language for governing the protocol and to create social consensus. Does the protocol have a formal governance process? How robust is the governance process and does it promote good governance?

Answer:

Users need to lock their tokens in the governance contract in order to participate in Tornado.Cash governance. A user needs at least 1,000 TORN to create a proposal. In the event that a user votes or creates a proposal, the tokens cannot be unlocked until the proposal execution period ends (8.25 days after proposal creation). Tokens can also be delegated to another address.

It is required that all proposals be smart contracts with verified code run from the governance contract). Using this method, any governance changes can be audited and tested. Proposals have a three-day voting period. There must be at least 25,000 TORN votes total for a proposal to succeed; if there are not enough votes, the proposal fails. The timelock for proposals is 2 days after they succeed. Once the time lock is released, any user can execute the proposal, initiating the changes. In the event that a proposal is not executed within 3 days, it will be considered expired and cannot be executed. All of Tornado.Cash's internal parameters can be changed by government proposals, including the implementation itself. The Governance process is robust and clearly defined here.

Score: 10

5. Regulatory

The Regulatory section describes the extent and quality of the regulatory environment that affects the Protocol. To be able to guarantee functionality, security, and legality the protocol should comply with regulatory requirements, or limit itself to facilitating services to users who are willing to operate outside of the traditional regulatory environment.

a) Does the protocol have any legal accountability? (15 points)

Does the protocol have any form of legal accountability? Can users and partners hold the protocol accountable in case of a breach of the agreement?

Answer: No legal structure is in place; the protocol is fully community owned and controlled.

Score: n/a

b) What is the quality of the legal jurisdiction? (10 points)

If the protocol has a legal entity, what is the quality of the jurisdiction the entity is established in? Will the jurisdiction be able to facilitate the legal framework for the protocol to expand while remaining accountable.

Answer: n/a

Score: n/a

About the Author: My name is Salomé and my background is in corporate audit & central banking and I have been involved in DeFi & Web3 for the past +2 years. Twitter handle: SalomeBernhart