

Smart Contract Audit Token Decentralized Autonomous Organization



Whitepaper

4/11/21

Written by
Eric Helms

Abstract

Smart Contract Audit Token Decentralized Autonomous Organization (SCAT DAO) is a new audit paradigm that reinvents the way audits are selected, performed, and financed. With SCAT DAO we solve audits inherent problem, the conflict of interest that comes from paying for an audit service. As we have seen with Enron, Tyco, and countless others, the possibility always exists for an auditor to commit fraud to keep their client happy. With SCAT DAO, the token holders choose the projects they care for and want audited. The audit process is standardized and performed by the community with all services funded by the DAO's treasury. SCAT DAO auditors are incentivized only to provide accurate audit results, regardless if the results are positive or negative. No more altering or softening results to appease clients. We are the client, we are the auditor, we are SCAT DAO.

Table of Contents

Introduction	3
How it Works	4
How is it Funded	9
Tokenomics	11
A Source of Trust for Cardano	14
What if Someone Doesn't Want to be Audited by SCAT DAO.	14
A Multi-Chain Future	15
Reinventing Other Industries	15
Value Proposition	16
Final Thoughts	17

Introduction

With an industry as nascent and technical as blockchain, mass adoption of decentralized applications (DApp), particularly dealing with Finance, will move slowly until enough trust has been generated with the general public. This can be done slowly as people cautiously use them and wait to see if any issues occur, or these applications can be independently audited using a consistent set of standards and provide a rating or certification on the code, assessment of the project's development team, and recommendation on its legitimacy. By creating this environment of trust, the DeFi ecosystem on Cardano will grow faster and attract a wider range of people.

The average user or investor does not have the technical expertise to read the code in a smart contract and understand if there is anything malicious included in it. Many people will want to participate in these applications, but lending any significant amount of crypto to an unverified application is unnerving for people, compounded by the fact that it is a decentralized entity that they cannot go to and complain to customer service. Without trust that these applications were written properly to do the things they promise, there will not be mass adoption.

But how can we trust a paid audit firm to be impartial? The answer is we cannot. We have seen Enron, WorldCom, Tyco, and countless other instances of paid auditors issuing fraudulent attestations to keep the client happy and continue earning audit and consulting fees. We also have hundreds of new Audit Firms popping up and performing smart contract audits which the public is unfamiliar with, have no history or reputation to draw on, and therefore not much faith can be placed in their results and opinion. We must create a new audit paradigm to change the way audits are chosen and paid for, as well as a trusted organization that the public can build a relationship with and have faith in the audit opinions it produces. The world is finally waking up to the need for decentralization and it is at the core of blockchain. So why would we accept our audit services meant to protect our investments coming from centralized organizations? Enter SCAT DAO (Smart Contract Audit Token Decentralized Autonomous Organization)

There needs to be Smart contract audit standards developed and consistently applied by independent decentralized organizations, which can apply a clear rating to the DApp and inform the public that they are safe to use. It needs to assess the code used in the smart contracts, assess the development team, including their backgrounds and history to determine if they have a history of rug pulls or other unscrupulous behavior. But more importantly, we need a decentralized DAO created which will have audit projects chosen by the community and funded entirely through their treasury, to avoid the conflict of interest that arises from paying an auditor for their service. A DAO that can be updated and molded by its community to adapt to any new unforeseen audit risks that may arise as the industry evolves and matures.

How It Works

Project Selection

The SCAT token is a governance token that holders will use to vote on which projects they would like to be audited. Anyone who holds a minimum of XX SCAT can propose an audit to be included for consideration in voting. There will be no minimum for voting, anyone who holds SCAT is eligible to vote and have a say in which projects they want to see audited. The DAO will determine the number of audit projects that it can perform each quarter, based on the total revenue being generated by the treasury and the total cost of each audit that will be calculated. We will audit the projects that receive the most votes from the community (1 SCAT = 1 vote).

Audit Methodology

We are currently developing the audit methodology and standards that will be used to assess the smart contracts and the development team who is responsible for creating the DApp. The goal is for these to become the industry standard so that all smart contract audits are conducted in a uniform manner. Once these are created, training materials will be developed so qualified candidates can easily follow and learn how to perform this work program on an audit. Also, this audit process is not meant to be unchanged or immutable. SCAT DAO will empower its community of auditors to propose changes and new best practices that they learn from performing the work. These updates or changes to the audit process can be voted on by the community and implemented. As Cardano and blockchain continue to evolve, we want the way to audit it evolve as well. Ensuring the best and most up to date methodologies are constantly being employed.

Who Performs the Work

We are in the process of developing training materials that will clearly outline our audit methodology and teach the work steps that need to be performed to complete the audit. Training materials will be available to everyone through our website and anyone can review this at their leisure to learn how to perform SCAT DAO audits (fluency in Haskell/Plutus will be helpful in successfully review the training materials). A test is also being developed that will assess a candidate's understanding of our audit methodology as well as their fluency of Haskell/Plutus. Upon successful completion of the training materials and receiving a passing score on the test they will receive a certification and be added to the listing of Qualified Candidates.

In addition to our knowledge review test, we are developing a scorecard that will assess a candidate's qualifications and determine if they have the necessary skills required to successfully perform an audit on behalf of the platform. This will consider their background, work history, knowledge of Haskell/Plutus, completion of Plutus Pioneers or similar programs, etc.. We care first and foremost that someone has the ability and knowledge vs blindly relying on professional certifications such as CPA, CFA, CA, etc. If they receive a passing score, they will be added to the listing of Active Available Auditors and are officially available to perform audits on behalf of SCAT DAO. Initially the SCAT DAO dev team will be reviewing these candidates to onboard them, but this responsibility will be transitioned to the new auditors based on the

number of successful audits performed with us. This is to ensure a clear and straightforward path to decentralization of the process away from the Dev team.

If an auditor becomes busy and would not have the availability to participate, they can deactivate themselves at any time and return to the Active listing whenever they become available. There will be no cap on the number of Active Available Auditors. If someone who self designates as available is chosen for an audit, an email will be sent to them and they will be required to accept the audit. If they cannot accept but designated as available, they will be put on hold for X number of audits. As auditors successfully complete audits and demonstrate their competency and trustworthiness, they will move up in ranking and will have different roles, responsibilities, and compensation based on their rank. It is outlined as follow:

Audits Performed	Rank	Compensation USD
0	Pawn	0
1	Pawn	X
2	Pawn	X
3	Knight	X * 1.5
4	Knight	X * 1.5
5	Queen	X * 2
10	King	X * 2.4

Each audit project that is voted on and selected by the community will be randomly assigned three auditors from the AAA listing. This will be 3 way blind so that none of the people are aware of each other or are able to communicate, which is meant to prevent collusion. Two people will independently perform the audit work program in its entirety and upload their results to the website repository when they are finished. The 3rd person will perform the Audit Quality Review (AQR). The AQR must review the work performed by the two auditors, ensure that both auditors have reached the same conclusions, and concur with their findings for the audit work to be completed. The redundancy of having 2 separate people perform the work and compare the results is meant to provide greater assurance that the testing was done correctly. If the work performed by the auditors does not match, the AQR will designate that in the system and the auditors will be notified. They will be required to go through the process over again, redo the work, and resubmit. This will be repeated until they can achieve matching results.

NOTE: We may initially have more than 3 auditors assigned to each audit in order to speed up the onboarding process. This will allow a large group of people to get multiple audits under their belt and progress to take over the additional responsibilities.

The system would be configured to always bring in 1 Pawn if available, so that new people can keep being onboarded into the program. It would also pull in 1 higher ranking individual as the second auditor (if available) and a Queen level would be required to perform AQR. This is to ensure that someone who is more experienced and has performed several audits on our behalf is

reviewing the work and ensuring its accuracy. If there is a situation where there were no new Pawns, two Knights or Queens can perform the work as well. At the completion of the audit work and AQR review, the AQR will ensure all workpapers have been uploaded to the website repository along with the results, and the closing process will begin.

As this is a community effort and to encourage the maximum number of people reviewing and concurring on the results, the community is incentivized to review the workpapers, results, and the smart contract to assess if the work was done properly and to see if any additional bugs or exploits can be found. For anything found, a new AQR will be randomly selected to review the claims and do another pass through of the workpapers and code. There will be a deadline for review and a certain percentage of votes will be required to certify the results and close the audit. Rewards are paid to the community for anything found and for participation according to the below table, and auditors are penalized as discussed in the next paragraph: (we are currently working to determine what rates to pay and will update in a future white paper).

At the successful completion of an audit, individuals will move up a level if their work was free from errors. If the AQR determines there were errors in the individuals work that would alter the opinion of a reasonable person, they would be dropped back down to the rank of Pawn 1. If someone feels that they did not make an error, 2 additional Queens will be selected to review and make a ruling. If they determine there was no error, the individual will continue to advance as normal and the Queen who made the incorrect call would drop back to Pawn 1. Initially the SCAT DAO team will perform the AQR role. As soon as there are auditors available who have performed the necessary number of successful audits to earn the Queen rank, this responsibility will begin transitioning to them and away from the Dev team, a clear and well-defined path to full decentralization.

After someone has successfully completed 10 audits, they would become a King. A King would have all of the responsibilities of a Queen, but would also be required to review incoming people and include them in the AAA listing. With each audit that they participate in, they would be required to review 10 new candidates as well (this will encourage constant and consistent growth). The candidates would be pulled from the system in the order that they applied. The Kings earn additional compensation for this additional effort, as outlined in the chart. If it is discovered that someone was admitted without the proper skills or rejected in spite of being qualified, the King would be bumped back down to Pawn 0 with a second infraction resulting in a permanent ban. Again, this will be performed by the Dev Team initially until sufficient Kings are available, a clear and well defined path to decentralization away from the Dev team and into the hands of the community.

At the completion of the audit work and closing process, the work performed will be uploaded to a repository on the website and results will be distributed through the website and available to all.

Auditors who perform an audit on behalf of SCAT DAO will receive a payment to compensate them for their time and effort. The compensation is outlined in the above table, and is meant to be very competitive to the industry. Auditors from all around the world who possess the required skills are encouraged to participate. The money will not be adjusted based on geographical location, which means an American Auditor and an Ethiopian Auditor would be compensated the exact same. This will hopefully encourage participation from the developing world where auditors are usually paid a fraction of what their western counterparts usually earn. In the spirit

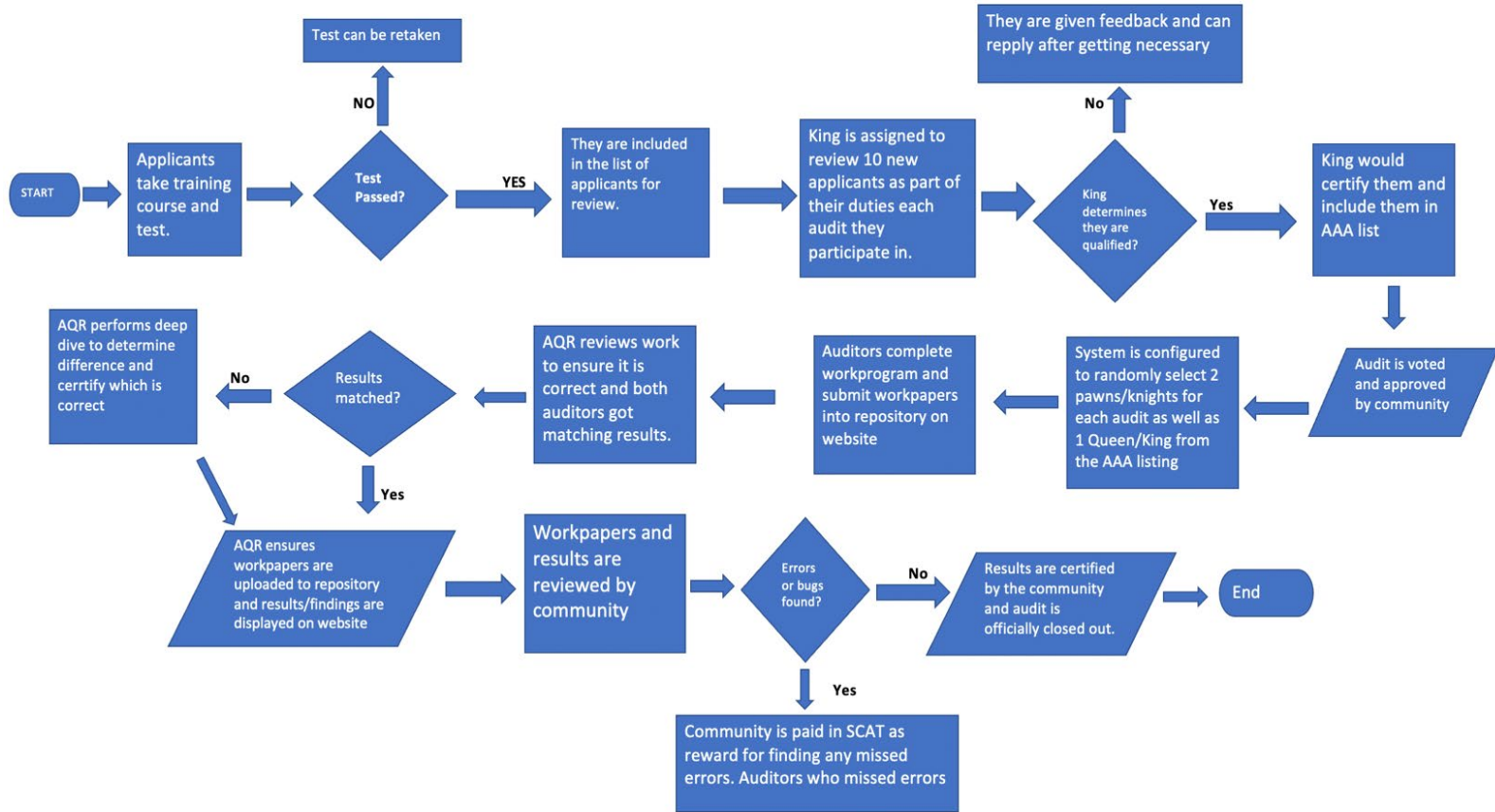
of Cardano, this project would like to empower audit professionals from all over the world with an opportunity to supplement their income, add to their resume, keep the Cardano community safe, and help build this new ecosystem.

Why Would people Want to Work on Behalf of SCAT DAO?

We intend to provide generous compensation above industry standards to the members of our community who perform audits on our behalf. As mentioned, this compensation will not be adjusted depending on geographical location. An auditor working in the United States or Europe will earn the same amount as an auditor in Africa or Southeast Asia. As the pay will be generous for US standards, we hope it will be especially rewarding for people who come from emerging markets. SCAT DAO is a global organization, and we want to tap into the vast amount of talent distributed throughout the globe.

SCAT DAO is not meant to be a full-time job. We are seeking individuals who can perform our work program and would like to supplement their income with some rewarding part time work on a project by project basis. Auditors who work on our behalf will get some excellence experience to add to their resume, can work from anywhere they choose, never have to commute or come into an office, and can dress however they like and work on their own schedule. Combining this with the rewarding compensation, the better question is, why wouldn't someone want to audit for SCAT DAO?

Process Flow Chart



How is it Funded

Treasury

SCAT DAO will never accept any money from any Dapp to audit their projects, the funding will be generated entirely by the investments that the treasury has made into various DeFi projects to generate a return. Initially, the plan is to provide liquidity to Decentralized Exchanges as the sole source of income. Liquidity providers are given a percentage of the fees the DEX generates through its trades. This will accomplish our need to generate income for operations while also creating sufficient liquidity for people who would like to trade our token. A big issue with new tokens that limits their ability to grow is a lack of liquidity. By providing the liquidity internally, we will ensure that people can buy and sell the token without creating wild price swings.

We have 30% of all tokens reserved for the SCAT DAO treasury. At the launch of SCAT DAO, half of those tokens (15%) will be sold and converted into either ADA or stable coin. When providing liquidity, you need to do it in pairs, so half SCAT and half ADA or stable coin. The treasury will not be able to provide liquidity if it only holds SCAT. This is why a sale to the general public will be necessary to generate the ADA to create the trading pair. Also, we want to make it clear that this will be a fair sale. No VCs or early investors gaining early access at a cheaper price. It will be the same price and access for everyone.

The income generated by these treasury investments will fund operations. Only DAPPS that have been audited by SCAT DAO will be eligible for investment. The CPAs with the SCAT DAO dev team will perform the initial audit for the DEX selected for its initial treasury investment.

Liquidity Pool Staking

SCAT DAO holders will be able to add trading pairs to our liquidity pools through our website. This will help increase the total liquidity in exchanges, increase the amount of income that the treasury is able to generate, and provide passive income to SCAT DAO holders. To reward SCAT DAO holders who choose to stake, they will receive 50% of the income generated from their stake, proportionally to the total amount invested, as well as a 5% APY reward paid in SCAT. If 50% of all tokens are staked, the treasury supply would hold enough to pay staking rewards for an 8-year period. After that period, the token holders can vote to pay staking rewards out of the excess treasury funds, or end staking rewards if they feel the treasury is robust enough to not require any additional staking to supplement itself.

Stake Pool

SCAT DAO will be setting up stake pools for three primary reasons. To assist and support Cardano's decentralization, to create an additional source of revenue to fund audit operations, and to distribute our tokens for free to the community. The first two points are fairly straightforward, but would like to make it clear that these stake pools are owned and operated by the DAO, not the Dev team. All revenue generated from it goes directly into the treasury to fund our audits. The last point is meant to be a way to distribute SCAT DAO to people who support the project and get tokens into as many hands as possible. We do not want the DAO to be controlled by early investors with deep pockets who can afford to buy as much as possible and have a disproportionate say in our operations. We would like the entire Cardano community to be involved and have a say in what we do. Therefore, anyone who stakes to our stake pool will still receive their regular staking rewards in ADA, but will also receive a bonus of SCAT DAO tokens as well. This will not be the typical Stake Pool Offering where we keep the ADA and give you our token in return. We feel that the normal revenue we earn from operating the stake pool is enough reward and keeping all of the ADA would be unfair to our supporters.

Tokenomics

Supply

We plan to mint 1 Billion Tokens and have it capped at that amount forever. No additional tokens can ever be minted. 1 Billion was chosen as it would allow for a lower price that the average investor could afford to participate in the DAO

Stake Pool Rewards

SCAT DAO cares deeply about the Cardano community and wants everyone to be involved in keeping it safe regardless of how much money they have to invest. Therefore, 15% of the tokens will be distributed for free through our stake pool. Initially, the hope was to distribute the tokens evenly to everyone with a Cardano wallet address to get the maximum number of people participating in SCAT DAO and avoid large whales holding large portions from the start and being able to unfairly influence the voting process. With the current minimum value to send Cardano Native Assets at about 1.5 ADA, it would be prohibitively expensive to distribute to every Cardano wallet. We have determined this is the best way to get free tokens into the hands of our supporters.

Treasury

As previously mentioned, Treasury is allocated 30% of tokens, 15% of which will need to be sold to create a trading pair, provide liquidity, and fund the treasury. Therefore, 15% of the total token supply will be sold through either an ICO, IDO, or ISO (currently in the process of determining best option). Also, to be clear this is to fundraise for the treasury only, this is not to generate funds for the developer team.

Staking Rewards

20% of the total supply will be held by the treasury to pay staking rewards. SCAT DAO holders will be able to stake a trading pair (SCAT and ADA) to the SCAT DAO treasury which the treasury will use to provide liquidity to exchanges. This will help increase the total liquidity in exchanges, increase the amount of income that the treasury is able to generate, and provide passive income to SCAT DAO holders. To reward SCAT DAO holders who choose to stake, they will receive 50% of the income generated from their stake, proportionally to the total amount invested, as well as a 5% APY reward paid in SCAT. If 50% of all tokens are staked, the treasury supply would hold enough to pay staking rewards for an 8-year period. After that period, the token holders can vote to pay staking rewards out of the excess treasury funds, or end staking rewards if they feel the treasury is robust enough to not require any additional staking to supplement itself.

Participation Rewards

X% of the total supply will be held to reward community participation in reviewing audit work and finding bugs/issues. We are in the process of determining what will be the best option and will update in a future white paper.

Development Team

The Development team has been allocated 25% of the total supply. Tokens for Dev Team will be vested over a 4 year period to assure investors there will not be a sell off that will suppress the price of the token at the expense of other investors. The tokens will be unlocked according to the following schedule:

- Product Launch: 1/5 of the tokens will be unlocked
- 365 days later: 1/5 of the tokens will be unlocked
- 365 days later: 1/5 of the tokens will be unlocked
- 365 days later: 1/5 of the tokens will be unlocked
- 365 days later: 1/5 of the tokens will be unlocked

Token Allocation

Development Team – 25%

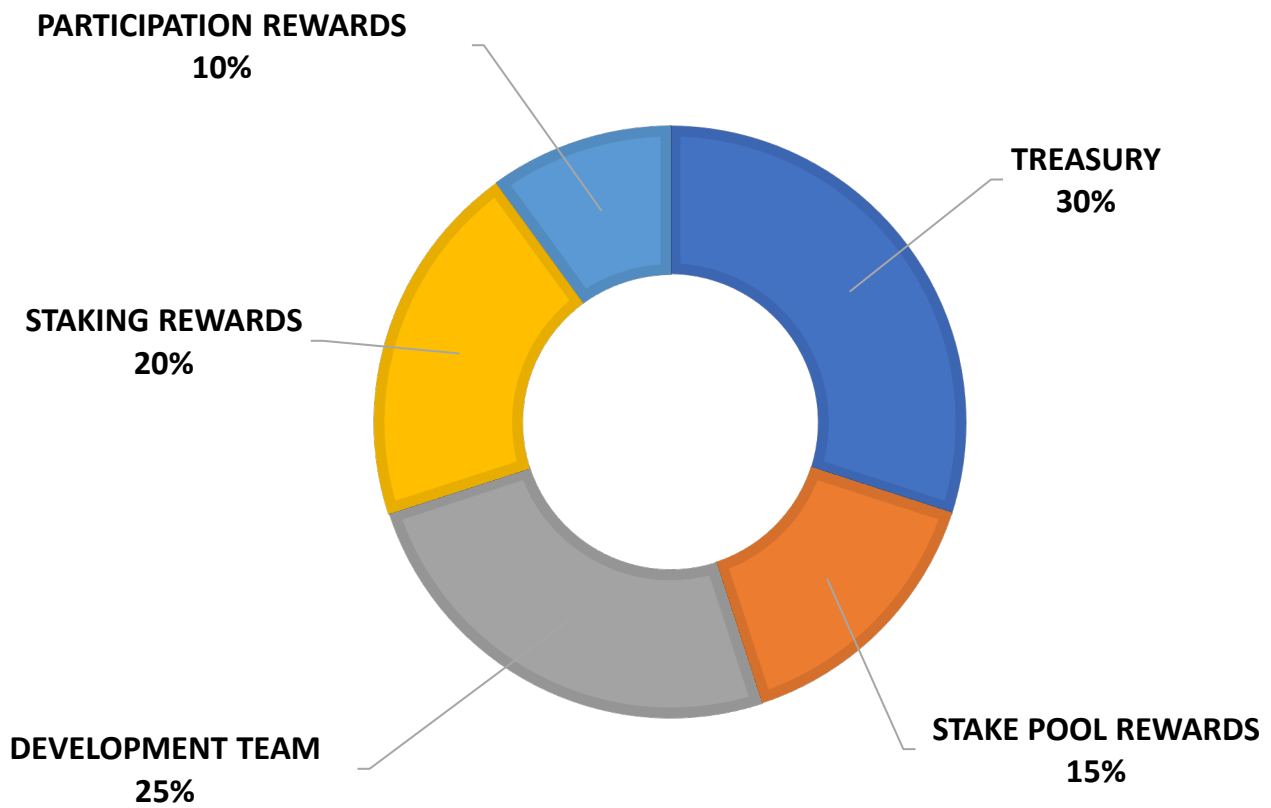
Treasury – 30%

Stake Pool Rewards – 15%

Staking Rewards – 20%

Participation Rewards – 10%

TOKEN ALLOCATION



A Source of Trust for Cardano

One of the primary goals for SCAT DAO is to be a trusted source where people go to begin their research on the Cardano Ecosystem. All projects that have been audited by the SCAT DAO will be listed on the website along with the rating based on the audit that was performed. The projects listed there will be the ones that the Cardano community has chosen because they are passionate about it and feel it is worthwhile. This combined with the fact that they have been audited and vetted and determined to be safe for investment, means being listed on the SCAT DAO website will provide a great deal of credibility for the applications.

It is a similar concept to having a Billboard top 100 where people looking for new music go to see what's popular at the time. But instead of music, it would be investors looking for projects to invest in, users looking for cool new applications to explore, or newcomers trying to learn more about what is available on Cardano. They would get unbiased information about them, assurance that the code is free of any bugs or malicious exploits, and an idea of the team that produced it and their credibility. As we have already seen on Ethereum and Binance Smart Chain, there are plenty of developers who are releasing products with bad intentions, meant to steal their investors money. Each time this happens, it hurts the credibility of those chains as well as blockchain in general. We all want to try and limit the likelihood of this happening on Cardano so that investors and users can trust what they are putting their money into and invest and use new products with confidence. Providing trust to the general public is why audit exists in the first place and SCAT DAO takes that to the next level by removing and possible conflicts on interest

What if Someone Doesn't Want to be Audited by SCAT DAO?

Traditionally, an applications Development Team will hire an auditor and grant them access to their code and anything else required to perform their job. Without this access, the auditors would have nothing to review. With SCAT DAO, we have changed the paradigm from products seeking to be audited to an audit collective choosing what they would like assurance over. Because of this, SCAT DAO would not have the same implied access to code and everything else that comes from being explicitly hired by someone. This presents a potential problem if the project chosen for audit does not want us to audit them and does not want to share their code with us.

There are some mitigating factors for this risk that lead us to believe it will not be a problem. With the blockchain revolution, many developers have chosen to build their projects open source, to allow everyone to learn from one another and advance the industry at a faster pace. We greatly admire all teams who chose to go this route, and SCAT DAO follows the same mentality by releasing all of our work and methodology freely as well. We expect this trend to continue and for a majority of products to have their code open to the public and available for us to review.

In addition, we expect inclusion in the list of applications covered by SCAT DAO to be a point of pride for most Dev Teams. Applications just starting up as well as established ones would likely welcome the added exposure and confidence that would come from being audited by the SCAT DAO, so even if a project was not open source, we would expect many of them to work with us to be able to perform the audit.

At the end of the day, being provided with a free comprehensive audit to give faith to the investing public is an easy sell. If for any reason an applications team did not want to be audited, that would be their decision and we would respect it. We would update the website to reflect that we could not cover them in our audit and the next highest voted project would take its place. As time passes and the SCAT DAO becomes more well known, we expect that a project passing on this opportunity would be a minority.

A Multi-Chain Future

SCAT DAO was created for Cardano, funded by project Catalyst, and will always have a strong connection and history with this blockchain. We are committed to this ecosystem and will always have a deep respect and admiration for it. We also feel that there will be many successful blockchains in the future that can and should all coexist with each other. We truly believe that this audit model is superior to the traditional model and that it should be adopted and implemented throughout the industry. Therefore in the future, SCAT DAO token holders will have the option to suggest other blockchains to expand to and vote to determine if that is what the community would like.

Reinventing Other Industries

We would like to point out that the actual audit work performed is the similar whether it is being done by a centralized entity or by SCAT DAO. We hope to create standardized methods that will be adopted within the industry, but most audits will follow a similar approach. The true difference is how the projects are selected and how they are financed. This means that this model can be imitated and followed for practically every other professional service that exists. We hope that SCAT DAO leads this revolution to change the way we think about and form Businesses going forward.

Value Proposition

Q: What can you do with the Token?

A: Owning the token gives the holder the right to submit proposals or suggestions that the community can vote on, vote on these proposals, and vote on which projects are selected for audit.

Q: Why would people want to buy it?

A: One of the primary goals for SCAT DAO is to be a trusted source where people go to begin their research on the Cardano Ecosystem. Having a project audited and listed on the SCAT DAO website will provide a lot of credibility and exposure for various dapps and projects and therefore be extremely desirable. This will create an incentive for developers to buy SCAT DAO in order to propose and vote on the projects for audit. The average investor will also realize the positive exposure to projects being covered by SCAT DAO and will want to have the projects they have invested in covered as well. They will need to buy and own SCAT to be able to propose and vote for those as well. There will also be people who believe in the work we are doing and wish to buy the token to support the project and help keep the Cardano ecosystem safe.

Q: Does it solve a problem?

A: Yes, a big one. The conflict of interest of audit firms accepting compensation directly from the client they are auditing has always seemed like a ticking time bomb. Anyone that has been in the industry has had to deal with, "How am I going to explain this to my client." We have seen Big 4 firms hiring the regulatory bodies that audit them, in order to try to go light on all of their other clients. It is a matter of time until the next Enron scenario plays out. It is not the Big 4 firms fault. At the end of the day, they have to keep the lights on. Instead, it is a flawed industry as a whole. At SCAT DAO, we hope to change the conflict of interest and give audit recommendations based on merit without worry of whether our client will rehire us. This is compounded by the current situation where there are hundreds of unknown companies performing smart contract audits without much history or reputation behind it. Someone could get an audit for their project, but if the company doing the audit is completely unknown, it doesn't provide much assurance. We are finally realizing the benefits of decentralization, so continuing to rely on centralized services for audits meant to keep us safe no longer makes sense. A new model is needed and SCAT DAO provides it.

Q: What if we need to make changes or improvements in the future?

A: Much like Cardano, SCAT DAO will have governance built in to allow for changes and updates as required. Token holders can propose changes that can be voted on by the community and then implemented. The world is constantly changing and having organizations that can change with it is crucial for continued success.

Final Thoughts

This Whitepaper outlines our general plans and methodology which we are currently tirelessly working to implement. As things progress, we may make changes to the process as we work through it. Any changes will be updated to the whitepaper immediately and a new version will be issued. In addition, the SCAT DAO is designed to grow and change with time. We are implementing methodology that we believe makes sense to begin with, but expect the community will want to suggest various improvements that can be voted on and implemented. SCAT DAO will draw on the relevant experiences of our community and together we will create the greatest audit organization the world has ever seen.