



DESSERT
FINANCE

Trippy Frens (TRIPPY)

ERC-721A Audit

Performed at block **14612926**

PERFORMED BY DESSERT FINANCE

CONTRACT ADDRESS: 0X822674BC21E35D4D79557335FB1CF679DD934500

CONTRACT ADDRESS: 0XF34D53F6425D44F554C9671F7E12C02A13E7C52F

INITIAL DISCLAIMER

Dessert Finance provides due-diligence project audits for various projects. Dessert Finance in no way guarantees that a project will not remove liquidity, sell off team supply, or otherwise exit scam.

Dessert Finance does the legwork and provides public information about the project in an easy-to-understand format for the common person.

Agreeing to an audit in no way guarantees that a team will not remove *all* liquidity (“Rug Pull”), remove liquidity slowly, sell off tokens, quit the project, or completely exit scam. There is also no way to prevent private sale holders from selling off their tokens. It is ultimately your responsibility to read through all documentation, social media posts, and contract code of each individual project to draw your own conclusions and set your own risk tolerance.

Dessert Finance in no way takes responsibility for any losses, nor does Dessert Finance encourage any speculative investments. The information provided in this audit is for information purposes only and should not be considered investment advice. Dessert Finance does not endorse, recommend, support, or suggest any projects that have been audited. An audit is an informational report based on our findings, We recommend you do your own research, we will never endorse any project to invest in.

Table of Contents



1. Contract Code Audit – Token Overview
2. ERC-721A Contract Code Audit – Overview
3. ERC-721A Contract Code Audit – Vulnerabilities Checked
4. Contract Code Audit – Contract Ownership
5. Contract Code Audit – Owner Accessible Functions
6. Contract Code Audit – Mint Functions
7. Website Overview
8. Social Media
9. Location Audit
10. Review of Team
11. Roadmap
12. Disclaimers

Contract Code Audit – Token Overview



Contract Code Audit - Vulnerabilities Checked

Vulnerability Tested	AI Scan	Human Review	Result
Compiler Errors	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow	Complete	Complete	✓ Low / No Risk
Integer Underflow	Complete	Complete	✓ Low / No Risk
Correct Token Standards Implementation	Complete	Complete	✓ Low / No Risk
Timestamp Dependency for Crucial Functions	Complete	Complete	✓ Low / No Risk
Exposed _Transfer Function	Complete	Complete	✓ Low / No Risk
Transaction-Ordering Dependency	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Variable	Complete	Complete	✓ Low / No Risk
Use of Deprecated Functions	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
State Variable Default Visibility	Complete	Complete	✓ Low / No Risk
Deployer Can Access User Funds	Complete	Complete	✓ Low / No Risk

The contract code is **verified** on EtherScan.

The vulnerabilities listed above were not found in the token's Smart Contract.

Contract Code Audit – Contract Ownership

Contract owner has been found.



The contract ownership is not currently renounced. **Ownership is required** for critical NFT functions.

We have placed the contract owner address below for your viewing:

[0x958c4edb417399bb9440dc2435de7fbd03b67176](https://etherscan.io/address/0x958c4edb417399bb9440dc2435de7fbd03b67176)

Contract Code Audit – Owner Accessible Functions

Function Name	Parameters	Visibility	Audit Notes
renounceOwnership		public virtual	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
transferOwnership	address newOwner	public virtual	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setAdmin	address user, bool isEnabled	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.

The functions listed above can be called by the contract owner.

If contract ownership has been renounced there is no way for the above listed functions to be called.

Contract Code Audit – Admin Accessible Functions

Function Name	Parameters	Visibility	Audit Notes
mint	address recipient, uint256 quantity	external	onlyAdmin modifier is detected. Admin can call this function at any time.
setInitialURI	string memory _initialURI	external	onlyAdmin modifier is detected. Admin can call this function at any time.
reveal	string memory baseURI_, bool _isRevealed	external	onlyAdmin modifier is detected. Admin can call this function at any time.
setBaseURI	string memory baseURI_	public	onlyAdmin modifier is detected. Admin can call this function at any time.

The functions listed above can be called by the Admin.

Contract Code Audit – Mint Functions

This Contract Can Mint New TRIPPY Tokens.



We do understand that sometimes mint functions are essential to the functionality of the project.

A mint function was found in the contract code. This is expected as NFTs will be minted on launch.

ERC-721A Contract Code Audit – Overview

Dessert Finance was commissioned to perform an audit on SaleERC721A

```
import "@openzeppelin/contracts/security/Pausable.sol";
import "@openzeppelin/contracts/security/ReentrancyGuard.sol";
import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/token/ERC721/extensions/ERC721A.sol";

/// @title TRIPPO Sale
/// @author @shubhamshin contact@shubhamshin.com
/// @notice NFT Sale contract for purchasing TRIPPO NFTs
contract SaleERC721A is ERC721A, Pausable, ReentrancyGuard {
    uint256 public price;
    uint256 public limit;
    uint256 public userLimit;
    uint256 public count;
    mapping(address => uint256) public userCount;

    event Purchased(address indexed user, uint256 quantity);
    event PriceUpdated(address indexed owner, uint256 price);
    event LimitUpdated(address indexed owner, uint256 limit);
    event UserLimitUpdated(address indexed owner, uint256 userLimit);

    constructor(
        uint256 _price,
        uint256 _limit,
        uint256 _userLimit
    ) {
        price = _price;
        limit = _limit;
        userLimit = _userLimit;
    }

    function setPrice(uint256 _price) public onlyOwner {
        price = _price;
        emit PriceUpdated(owner(), _price);
    }

    function setLimit(uint256 _limit) public onlyOwner {
        limit = _limit;
        emit LimitUpdated(owner(), _limit);
    }

    function setUserLimit(uint256 _userLimit) public onlyOwner {
        userLimit = _userLimit;
        emit UserLimitUpdated(owner(), _userLimit);
    }

    function purchase(uint256 quantity) private {
        require(msg.sender, quantity);
        count = count + quantity;
        userCount[msg.sender] = userCount[msg.sender] + quantity;
        emit Purchased(msg.sender, quantity);
    }

    function purchase(uint256 quantity)
        external
        payable
        whenNotPaused
        restrictForPhase
        nonReentrant
    {

```

Contract Address

0xF34D53f6425d44f554c9671F7E12c02a13E7c52f

Contract Creator

0x8a7b03380a62afe061edeb3abb0ca80c26f05681

Source Code

Contract Source Code Verified

Contract Name

SaleERC721A

Other Settings

default evmVersion

Compiler Version

v0.8.7+commit.e28d00a7

Optimization Enabled

Yes with 100 runs

Code is truncated to fit the constraints of this document.

[The code in its entirety can be viewed here.](#)

Contract Code Audit - Vulnerabilities Checked

Vulnerability Tested	AI Scan	Human Review	Result
Compiler Errors	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow	Complete	Complete	✓ Low / No Risk
Integer Underflow	Complete	Complete	✓ Low / No Risk
Correct NFT Standards Implementation	Complete	Complete	✓ Low / No Risk
Timestamp Dependency for Crucial Functions	Complete	Complete	✓ Low / No Risk
Exposed _Transfer Function	Complete	Complete	✓ Low / No Risk
Transaction-Ordering Dependency	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Variable	Complete	Complete	✓ Low / No Risk
Use of Deprecated Functions	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
State Variable Default Visibility	Complete	Complete	✓ Low / No Risk
Deployer Can Access User Funds	Complete	Complete	✓ Low / No Risk

The contract code is **verified** on EtherScan.

The vulnerabilities listed above were not found in the token's Smart Contract.

Contract Code Audit – Owner Accessible Functions

Function Name	Parameters	Visibility	Audit Notes
renounceOwnership		public virtual	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
transferOwnership	address newOwner	public virtual	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setAdmin	address user, bool isEnabled	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setPhase	Phases _phase	external	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setPrice	uint256 _price	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setLimit	uint256 _limit	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.
setUserLimit	uint256 _userLimit	public	onlyOwner modifier is detected. Owner can call this function if the contract is not renounced.

The functions listed above can be called by the contract owner.

If contract ownership has been renounced there is no way for the above listed functions to be called.

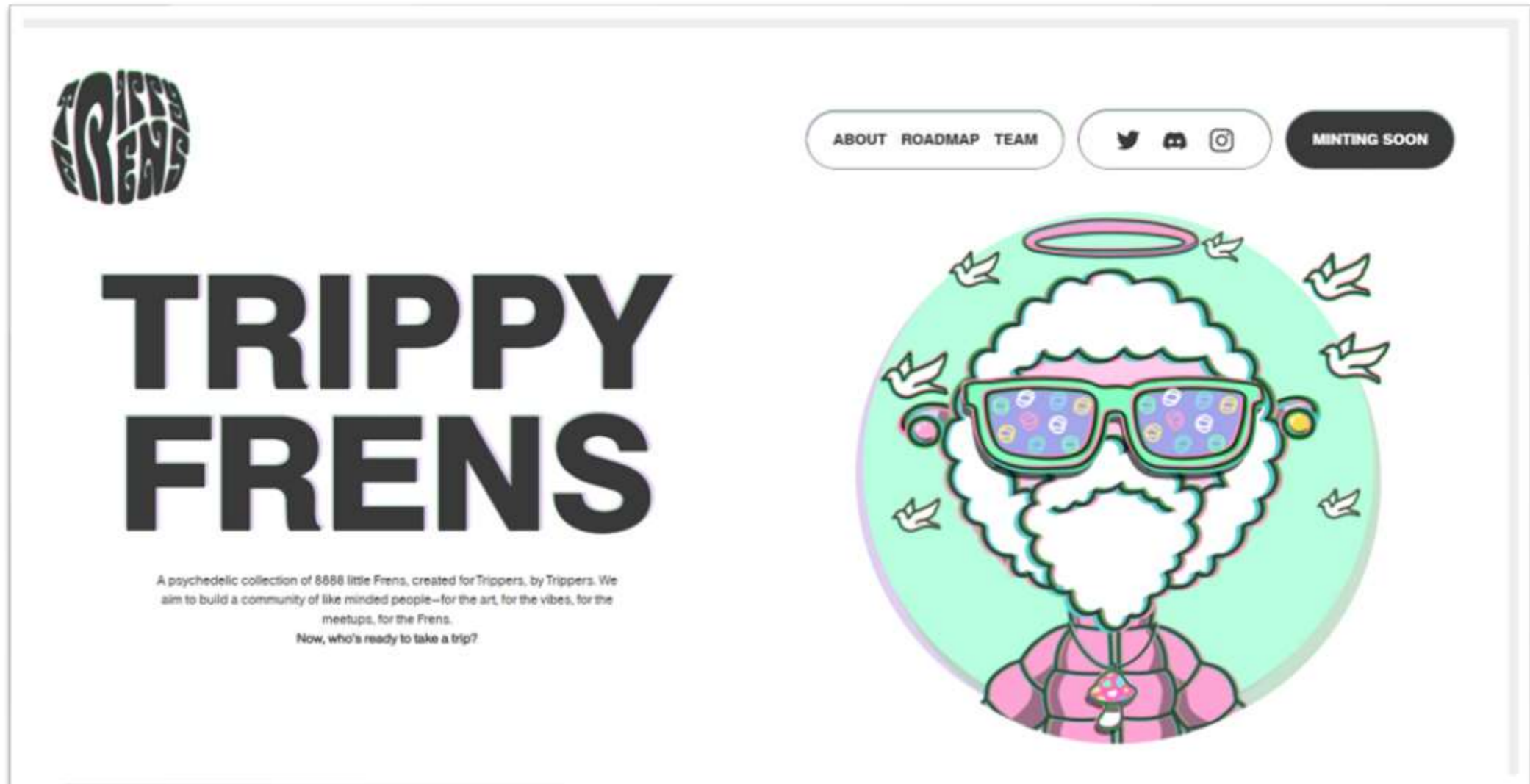
Contract Code Audit – Admin Accessible Functions

Function Name	Parameters	Visibility	Audit Notes
setWhitelist	address user, bool _isWhitelisted	public	onlyAdmin modifier is detected. Admin can call this function at any time.
batchSetWhitelist	address[] memory users, bool[] memory _isWhitelisted	external	onlyAdmin modifier is detected. Admin can call this function at any time.
pause		external	onlyAdmin modifier is detected. Admin can call this function at any time.
unpause		external	onlyAdmin modifier is detected. Admin can call this function at any time.

The functions listed above can be called by the Admin.

Website Part 1 – Overview

www.trippyfrens.com



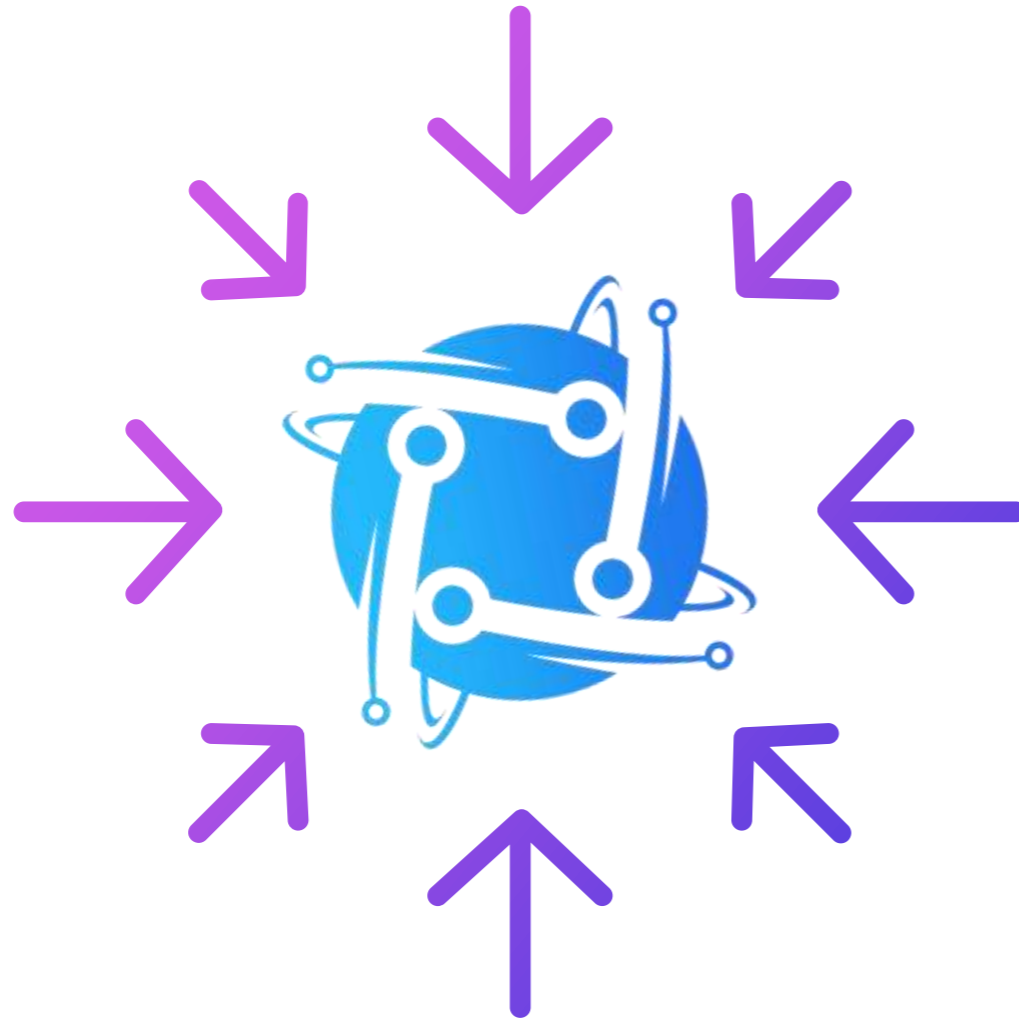
Above images are actual snapshots of the current live website of the project.

Website was registered on 03/06/2022, registration expires 03/06/2025.

✓ This meets the 3 year minimum we like to see on new projects.



Website Part 2 – Checklist



- ✓ Mobile Friendly
- ✓ No JavaScript Errors
- ✓ Spell Check
- ✓ SSL Certificate

The website contained no JavaScript errors. No typos, or grammatical errors were present, and we found a valid SSL certificate allowing for access via https.

No additional issues were found on the website.

Website Part 3 – Responsive HTML5 & CSS3

No issues were found on the Mobile Friendly check for the website. All elements loaded properly and browser resize was not an issue. The team has put a considerable amount of thought and effort into making sure their website looks great on all screens.

No severe JavaScript errors were found. No issues with loading elements, code, or stylesheets.



Website Part 4 (GWS) – General Web Security



SSL CERTIFICATE

A valid SSL certificate was found. Details are as follows:

Offered to: trippyfrens.com

Issued by: cPanel, Inc.

Valid Until: 07/10/2022



CONTACT EMAIL

A valid contact email was found on the official website. Contact email is listed as shown below:

[Contact](mailto:hi@trippyfrens.com)

hi@trippyfrens.com



SPAM / MALWARE / POPUPS

No malware found

No injected spam found

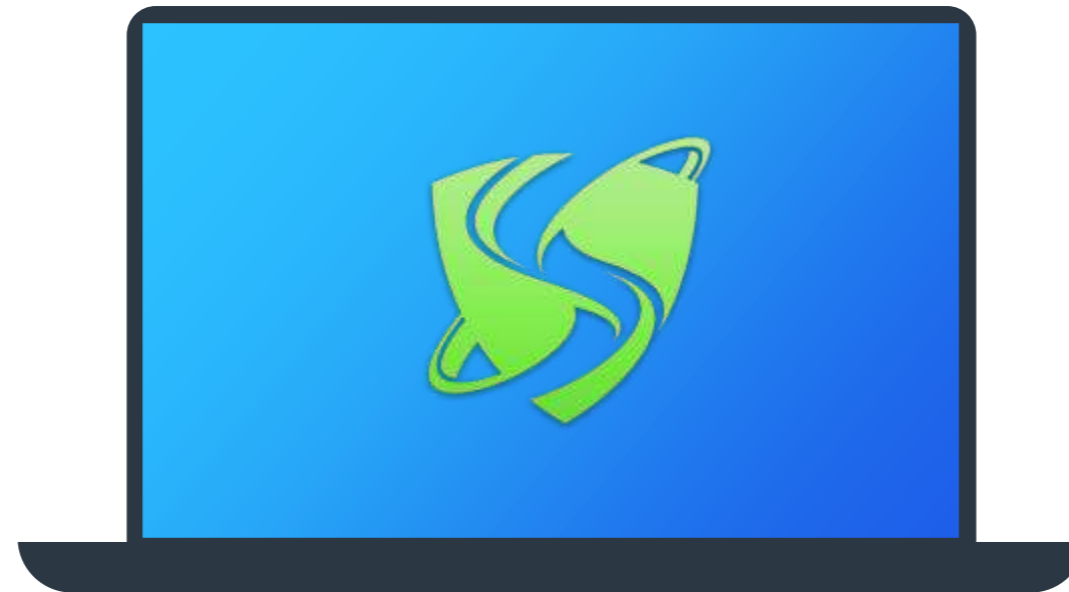
No internal server errors

No popups found

Domain is marked clean by Google, McAfee, Sucuri Labs, & ESET



Social Media

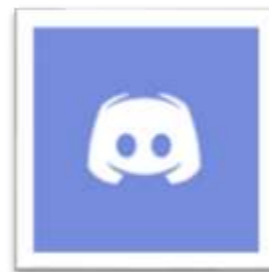


We were able to locate a variety of Social Media networks for the project.

All links have been conveniently placed below.



[Twitter](#)



[Discord](#)

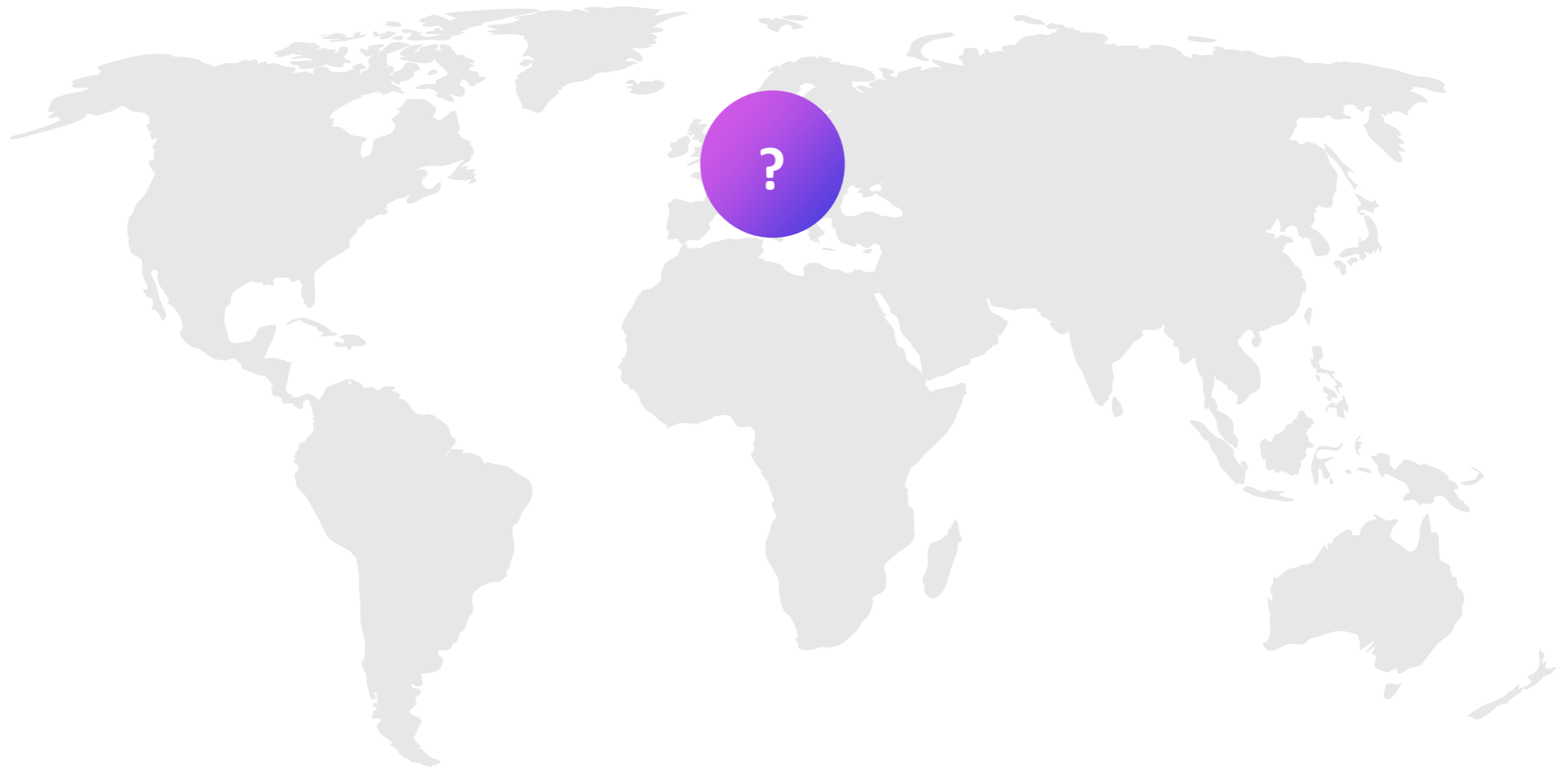


[Instagram](#)

✓ **At least 3 social media networks were found.**

Location Audit

We were unable to identify a primary location for the project at this time or a location has not been declared.



Team Overview

The following information about the team has been found on the projects website.

THE INCREDIBLY AWESOME TRIPPY FRENS TEAM.



CT

Founder/Community Builder. A 10 year veteran of the TV industry. Building Web 3 bridges between community, art, and entertainment.



TOSHIRO

Art Department Head. A psychedelic mind, and an eye for beauty. Trippy Frens is the result of Toshiro's vision.















DANILAB

Lead Designer. Multidisciplinary design genius. This guy can literally do anything. From animation, to design, to website building. Danilab is a master of his craft.



Team Overview

The following information about the team has been found on the projects website.

		
<p>REYMARTIN</p> <p>2D Artist. Reymartin's art continues to inspire, while driving the fervor within the community. Without Rey's concepts, there are no Trippy Frens.</p> <p></p>	<p>JERIK</p> <p>3D Artist. The man behind the psychedelic 3d holder's collection. Supremely talented, and infinitely motivated, Jerik can't be stopped.</p> <p></p>	<p>SAIPAX</p> <p>God Emperor Of Discord. There is no one more diligent when it comes to security than Saipax. A discord wizard with a hilarious Polish sense of humor.</p> <p></p>
		
<p>STEVERINO</p> <p>Collab Manager. Slides into dms faster than a Tesla on a straightaway. Enjoys fine tequilas and mutual beneficial collaborations.</p> <p></p>	<p>DK</p> <p>Community builder. An absolute mad lad, but a genius at nurturing relationships with other NFT communities.</p> <p></p>	<p>BUSY</p> <p>Lead Mod and Meme Pusher. If you've been in our discord, then Busy has probably insulted you with a well-timed meme.</p> <p></p>

Roadmap

A roadmap was found on the official website, we have conveniently placed it on this page for your viewing.

**WE HAVE BIG PLANS FOR TRIPPY FRENS,
AND WE'RE SO EXCITED TO HAVE YOU
ALONG FOR THIS MAGICAL RIDE!**

- 1. FREE MINT OF 3D TRIPPY FRENS FOR HOLDERS OF 3 OR MORE
2D TRIPPY FRENS Q2 2022**
- 2. FREE MERCH DROP Q2 2022**
- 3. IRL EVENT AT NFT NYC + MAJOR ANNOUNCEMENT Q2 2022**
- 4. ROADMAP 2.0 Q3 2022**
- 5. IRL TRIPPY EVENT IN THE NEVADA DESERT Q4 2022**
- 6. HOT BOX 3D EXPERIENCE COMING Q4 2022/Q1 2023**

Disclaimer



The opinions expressed in this document are for general informational purposes only and are **not intended to provide specific advice or recommendations for any individual or on any specific investment**. It is only intended to provide education and public knowledge regarding projects. This audit is only applied to the type of auditing specified in this report and the scope of given in the results. Other unknown security vulnerabilities are beyond responsibility. Dessert Finance only issues this report based on the attacks or vulnerabilities that already existed or occurred before the issuance of this report. For the emergence of new attacks or vulnerabilities that exist or occur in the future, Dessert Finance lacks the capability to judge its possible impact on the security status of smart contracts, thus taking no responsibility for them. The smart contract analysis and other contents of this report are based solely on the documents and materials that the contract provider has provided to Dessert Finance or was publicly available before the issuance of this report (issuance of report recorded via block number on cover page), if the documents and materials provided by the contract provider are missing, tampered, deleted, concealed or reflected in a situation that is inconsistent with the actual situation, or if the documents and materials provided are changed after the issuance of this report, Dessert Finance assumes no responsibility for the resulting loss or adverse effects. Due to the technical limitations of any organization, this report conducted by Dessert Finance still has the possibility that the entire risk cannot be completely detected. Dessert Finance disclaims any liability for the resulting losses.

Dessert Finance provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Even projects with a low risk score have been known to pull liquidity, sell all team tokens, or exit-scam. Please exercise caution when dealing with any cryptocurrency related platforms.

The final interpretation of this statement belongs to Dessert Finance.

Dessert Finance highly advises against using cryptocurrencies as speculative investments and they should be used solely for the utility they aim to provide.



Thank You

DESSERT FINANCE PROJECT AUDIT HAS BEEN COMPLETED FOR TRIPPY FRENS (TRIPPY) 1 DSRT HAS BEEN SENT TO AUDITED PROJECT'S CONTRACT ADDRESS FOR VERIFICATION OF THIS AUDIT AT BLOCK NUMBER: **14612926**

THIS AUDIT IS ONLY VALID IF VIEWED ON [HTTPS://WWW.DSSERTSWAP.FINANCE](https://www.dessertswap.finance)

www.dessertswap.finance
<https://t.me/dessertswap>