



TOWER OF MATC GAME SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS

AUDIT REPORT



NOVEMBER 13, 2023

WWW.THECRYPTOAUDIT.COM

Audit Report:-

Disclaimer:

This audit is only to the Smart-Contract code at the specified address!

Thecryptoaudit is a 3rd party auditing company that works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration are fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Thecryptoaudit.

Investors are not in any way obliged, coerced, or influenced to invest in projects audited by Thecryptoaudit.

We are not responsible for your funds or guarantee you profits.

We highly recommend that investors do their own research and gain crypto experience before investing

To report any scam, malpractices and irregularities, please send a message via Telegram to <https://t.me/thecryptoaudit> for blacklisting.

Conclusion:

The **TOMG** Smart-Contract found no vulnerabilities, no backdoors, and no scam scripts.

The code was tested with compatible compilers and simulated manually reviewed for all commonly known and specific vulnerabilities.

So, **TOMG** Smart-Contract is safe for use in the Polygon main network.

Smart contract information:

- TOMG
 - Contract Name: TOMG
 - Compiler Version: v0.8.20+commit.a1b79de6
 - Optimization Enabled: Yes with 200 runs

Deploy information:

- Deploy date: Nov-11-2023 06:45:27 PM +UTC
- Deploy block number: 49823658
- Deployer address:
 - [0xa9414B016cAE69b90490685C31DA3a26F0893bb1](#)
- Deploy transaction hash:

- 0x9d5011f40964218f32abfcbc5f8d4542bf01c24e276991a428a570507ee46b4c

Contract Overview Checklist

The code was tested with compatible compilers and simulated manually reviewed for all commonly known and specific vulnerabilities.

Vulnerability description	status
Visibility of functions and variables	Passed
Compiler error	Passed
ROI Investment Plan	Warning
Transfer Block	Passed
Floating pragma	Passed
Timestamp dependence	Passed
Deprecated solidity functions	Passed
Gas limit and loops	Passed
Front running	Passed
User balance manipulation	Passed
Dos with revert	Passed
Dos with block gas limit	Passed
Reentrancy security	Not used
Malicious libraries	Passed
Integer overflow/underflow	Passed
Using inline assembly	Passed
Missing event emission	Passed
Missing zero address validation	Passed
Use of tx.origin	Passed
Oracle security	Passed
Outdated compiler version	Passed

Block values as a proxy for time	Passed
Presence of unused code	Passed
Data consistency	Passed
Money giving bug	Passed
Unnecessary use of SafeMath	Warning
Self-destruct interaction	Passed
Signature unique id	Passed
Weak sources of randomness	Passed
Optimize code and efficient gas fee	Warning

CRITICAL ISSUES	(Critical, high severity)	0
HIGH ISSUES	(High, medium severity)	1
ERRORS, WARNINGS	(Medium, low severity)	0
OPTIMIZATION	(Low severity)	0
RECOMMENDATIONS	(Very low severity)	0

High ISSUE

The system used is called ROI and must be considered HIGH-RISK.

Users' principal deposits cannot be withdrawn. Users can get dividends and referral commissions. Dividends are paid from deposits of other users. Do always invest with proper knowledge and investigation.

Independent description of the smart-contract functionality

The **TOMG** smart contract provides the opportunity to invest **USDT** from 50 USDT in the contract and get a 115% return on investment between 10 to 40 days if the contract balance has enough funds for payment.

- v. All dividends are calculated at the moment of request and available for withdrawal after freeze time.
- v. Each subsequent deposit is kept separately in the contract to maintain the payment amount for each deposit.

Launch Date: Wed Nov 15 2023 12:00:00 GMT+0000

Contract Owners Fee

withdraw Fee: 7%

INVESTMENT PLAN

- In order to make a deposit, the user must first register.
- The minimum deposit amount is 50 USDT
- The maximum deposit amount for the first deposit is 500 USDT
- The maximum deposit amount is 3000 USDT
- The amount of the deposit must be a multiple of 50. For example, 100, 150, 200, and...
- The amount of each user's deposit must be greater than the amount of the user's previous deposit.
- 5% of the deposit amount as a bonus is given to the user on the first deposit, and he can withdraw it along with other rewards in his withdrawals.
 - This bonus is only for the users who deposit with USDT, not from a split balance.
- When the user makes a deposit, that deposit is frozen for a minimum of 10 days and a maximum of 40 days.
- The freeze time of the first deposit is ten days, and 24 hours are added to the frozen amount for each subsequent deposit.
- If the deposit is of split type and the freeze feature has been activated at least once, or the freeze feature is inactive and the time of the user's first deposit is less than the time of the activation of the last freeze feature, the user's deposit will be frozen for 40 days.
- Limitation of new users in the project:
 - On the first day of the project, five new users can deposit, and for every two days that pass from the launch of the project, one user is added to this limit. For example, on the third day, a maximum of 6 new users can deposit.
 - After 365 days from the launch of the project, this restriction will be deactivated.

- There is a function in the contract called "redeposit" that users can Redeposit with the amount of the last deposit they made.
- Cycle max deposit rules:
 - After the launch of the project, every ten days, there is a limit for the deposit amount.
 - The minimum amount to deposit is 50 USDT, and the maximum is 500 USDT for the first deposit.
 - In the next deposit, If the freeze feature is active:
 - If the user's total freezed amount is greater than the user's total revenue, the minimum deposit amount will be 150% of the user's previous deposit amount; otherwise, it will be 200% of the user's previous deposit amount.
 - If this case maximum deposit amount will be calculated as follows:
 - $3000 \text{ USDT} * (2 ^ \text{the number of times the freeze feature is activated})$

The calculation of the profit of the user's deposits is done in the deposit function.

- - After the freeze time of each deposit, the user can add the original amount of the deposit and 15% profit to his withdrawable amount by making a new deposit.
 - At the time of withdrawal, **30% of the user's profit** is added to the user's **split balance**, and **3% of the user's profit** is added to the predict **pool**, the uses of which are explained below. Based on this, **the approximate percentage** of return to the user will be **109%**.
- In each withdrawal:
 - 30% will be added to the split balance
 - 7% will be sent to the owner's wallet
 - 3% will be added to predict pool
- The 3% percentage transferred to the predict pool, and the owner fee is calculated from the user's main deposit profit plus the user's referral profit (from levels 1 to 4) plus the bonus earned from predict.
- The 30% that goes to the split balance is from the final withdrawal amount of the user minus the admin fee and the amount transferred to the predict pool.

Split Balance

Users can transfer their split balance to a new wallet and make a new deposit with the received split balance and receive profit again.

- The user can transfer split with the "transferBySplit" function.
- The user must make his deposit with the "depositBySplit" function.
- The receiver wallet can only run the "depositBySplit" function if he has **not made a deposit yet**.
- A new deposit will be made by split balance, and no need to send any more USDT.

- In transfer by split, a 10% fee is charged from the sender; for example, if the user wants to transfer 100 USDT, he must have 110 USDT in his split balance, and 100 USDT will be sent to the destination, and 10 USDT will be charged as a fee.
- The minimum amount to deposit by split and deposit by split is 100 USDT, and the amount must be a multiple of 100.

Predict

After the launch of the project, every day that the project moves forward, a predict round will be held in the first 30 minutes of the day, and 20 users in that day who participate in this predict round will win a prize.

- At the end of each day, prizes are distributed among 20 winners, and the prize amount is added to the user's withdrawable amount.
- At the time of participating in each round, the user must enter an amount. When the prizes are distributed, the prize list will be filled as follows:
 - The number of 50 USDT deposits that occurred on the previous day is placed as the first winning number, and if the number of winners is less than 20, one unit is subtracted from the number of new users of the previous day, and this process continues until the list reaches 20 or the number 50 USDT deposits from the previous day reaches zero.
- The cost of participating in the prediction round is 1 USDT, and the user must pay it directly.
 - At the time of withdrawal, 3% of the withdrawable amount is added to the predict pool.
- The prize is paid from the predict pool.
- Each user can participate in each round for a maximum of 10 times.
- Prize amount of each winner:

Winner level	Prize percentage from the predict pool
1	30%
2	20%
3	10%
4	5%
5	5%
6	2%
7	2%
8	2%
9	2%
10	2%
11	2%
12	2%
13	2%
14	2%
15	2%

16	2%
17	2%
18	2%
19	2%
20	2%

Withdraw

All profits that the user gets from daily rewards, as well as referral and deposit profits, are added to the user's withdrawable amount, and the user can withdraw them without a time limit.

- In each withdrawal:
 - Profit is 15%
 - 30% (4.5% of 22.5%) transfer to the split balance of the user
 - 7% (1.05% of 22.5%) transfer to the owner's wallet
 - 3% (0.45% of 22.5%) transfer to the predict pool
 - 60% (9% of 22.5%) transfer to the user's wallet as profit
 - The capital amount is 100% deposited amount

Freeze Reward

If the freeze reward feature is activated, the user's calculated profit after unfreezing the deposit is as follows:

- If the user's total frozen amount is more than the total amount of profit that has been added to the user's withdrawable amount, the user's profit after unfreezing is obtained from the difference between the user's total frozen amount and the user's total revenue amount.
- When the freeze feature is active, the freeze time of each cycle is calculated based on the maximum of 40 days for users who have deposited.
- This feature is disabled when the project is launched.

How to activate and deactivate the freeze reward feature:

The contract has a balance status that changes with each deposit based on the following table.

ID	Minimum balance required
1	$X \geq 500000$ USDT
2	$X \geq 1000000$ USDT
3	$X \geq 2000000$ USDT
4	$X \geq 5000000$ USDT
5	$X \geq 10000000$ USDT

After each withdrawal and deposit, if the contract balance falls below the value shown in the table below for each level, this feature will be activated, and if the

contract balance is equal to or greater than the recovery value again, this feature will be disabled again.

ID	Balance to activate the freeze	Recovery amount required
1	$X < 350000$ USDT	$X \geq 800000$ USDT
2	$X < 700000$ USDT	$X \geq 1500000$ USDT
3	$X < 1000000$ USDT	$X \geq 2000000$ USDT
2	$X < 3000000$ USDT	$X \geq 5000000$ USDT
3	$X < 5000000$ USDT	$X \geq 10000000$ USDT

Referral System (Match Bonus)

- The referral should be an active user; it means the referral address has at least one deposit.
- To register, the user must have a valid referrer or use the project account as a referrer.
- The referral bonus is distributed up to 20 levels.

User Star (Referral Levels)

The user's star is calculated based on the following table

level	Last user investment required	Number of referrals required	Maximum team turnover required	Other team turnovers required
1	$x \geq 50$ USDT	0	0	0
2	$x \geq 500$ USDT	0	0	0
3	$x \geq 1000$ USDT	0	0	0
4	$x \geq 2000$ USDT	50	10000 USDT	10000 USDT
5	$x \geq 3000$ USDT	200	20000 USDT	20000 USDT

Guide:

- **Maximum team turnover** = The total amount of direct referred deposit with the highest amount + The total freed amount referred by the direct referrer with the highest amount
- **Other team turnover** = The difference between Maximum team turnover with other direct referrals
- Number of referrals = number of referrals up to 20 levels

How to distribute referral commission:

All commission percentages are calculated based on the reward amount.

- In order for the commission interest to be paid to the upline, the upline user must have an active deposit.
- The reward amount is equal to the user deposit amount.
 - The **maximum** amount with which the reward is calculated is the amount of the **last active deposit** of the upline user.
- In order for the referrer to receive referral profit, the profit level must be one, or the referrer level must be equal to or more than four, and the profit level must be less than 4. For example, in order to receive referral profit at level 3, the user must be a 4 or 5 star user.
- Conditions for calculating the referral profit for the referrer in each deposit (one of the following conditions must be met for the referrer to receive the referral benefit).
 - The freeze reward feature must be disabled.
 - The user's total frozen amount must be greater than the user's total revenue amount.
- If the above conditions do not occur during the calculation of profit, if the referrer level is 5, the commission will be added to the variable, and the user can add it to his withdrawable amount with the next investment.

Referral bonus distribution table:

level	percentage of the reward amount
1	5%
2	1%
3	2%
4	3%
5	2%
6	1%
7	1%
8	1%
9	0.5%
10	0.5%
11	0.5%
12	0.5%
13	0.3%
14	0.3%
15	0.3%
16	0.3%
17	0.3%
18	0.3%
19	0.3%
20	0.3%



END OF AUDIT REPORT

