

# **GuardianChain White Paper**

## *A Decentralized Approach to Cryptoasset Theft Recovery*

### Abstract

The ascent of cryptoassets has paralleled the rise in associated thefts. While centralized systems offer mechanisms for fraud detection and resolution, the decentralized nature of blockchain necessitates unique solutions.

GuardianChain, built on the Ethereum network and utilizing an ERC20 token, GuardToken, introduces a method for marking suspicious transactions, ensuring a mechanism for theft recovery.

### **1. Introduction**

With growing adoption, cryptoassets are increasingly becoming targets for illicit activities. GuardianChain proposes a decentralized mechanism for users to mark, track, and recover stolen assets, combining community-driven verification with an incentivized model for participation.

### **2. Technical Architecture**

#### 2.1 The Marking Process

*Proof of Theft:* The system relies on victims obtaining evidence of unauthorized transactions. This proof is essential for securing the marking process past 48-hours. This time limit may be extended in order to accommodate people who may not be tech-savvy or who may not notice the theft immediately. This could be done by extending the timeframe or offering a tiered system, where an immediate response might require a smaller fee and a later claim requires a higher fee.

*GuardToken:* To activate the marking mechanism, users must possess or procure GuardTokens worth approximately 50€. These tokens enable the deployment of a marking contract on the GuardianChain, and will be distributed to validators upon successfully agreeing by consensus on the merits of a claim. In the future, a sliding scale fee system will be implemented, and will be based on the value of the claim, ensuring accessibility for claims of all sizes.

*Automatic Marker Creation:* Once the initial GuardTokens were paid, the system generates a unique cryptographic marker, linked directly to the suspicious transaction's hash.

*Claims staking :* A user must also stake 500€ worth of GuardTokens within 24 hours, otherwise the claim will not be submitted to validators, and the marker will be removed after a 48-hour period. This amount will be locked until the case is fully resolved. In the event of a wrongful or unsubstantiated claim, the stake will be slashed and burned. If the claim is approved, the stake will be fully restored to the user.

#### 2.2 Tracking Mechanism

*Ethereum Smart Contracts:* Leveraging Ethereum's proven smart contract capability, the marker follows the fund's path, updating its state with every movement or transfer.

*Public Blockchain Integration:* Integration with other public blockchains requires them to recognize and respond to GuardianChain's markers. A standard API or a set of smart contract interfaces would facilitate this interoperability. Exchanges and crypto-asset wallets should include a notification

feature, to notify a user of funds that were marked as stolen. The limitations can be tailored to the status of the marked funds (claim initiated, claim approved, counter-claim rejected) and include: making it more difficult to move the funds (forcing multiple smaller transactions or time delays), asking for extra KYC before moving the funds, further restrictions to certain services, notifying another wallet that the funds they are about to receive are marked as being stolen).

### 2.3 Verification and Validation

*Validator Nodes:* Selected nodes on the GuardianChain, known as validators, are responsible for reviewing and validating the legitimacy of theft claims.

*Staking Mechanism:* To act as a validator, nodes need to stake a certain amount of GuardTokens. This stake is a commitment to the honest evaluation of claims.

*Consensus Mechanism :* GuardianChain employs a unique consensus method. All validators must reach unanimous agreement on a claim's legitimacy. Any dissenting node, against the majority consensus, incurs a penalty, losing a fraction of their staked GuardTokens. Validators can refuse to vote on the merit of a claim. Each claim must include at least 5 validators. If there aren't enough validators that agree to vote on the claim, the claim is dismissed and half of the 500€ stake is returned to the user/victim. The other half is kept until the suspected thief has had a chance to submit a counter-claim, and is returned in case the counter-claim fails. To prevent centralization of the decision making process, GuardianChain will reflect on the introduction of a tiered system where smaller decisions require simple majorities and more significant decisions demand higher consensus percentages (for instance, depending on the amount stolen).

*Counter-Claim Mechanism:* Once an individual, whose assets are marked due to suspected theft, is notified of the marker, they can initiate a counter-claim asserting their legitimate ownership of the assets. To proceed, they must also acquire GuardTokens equivalent to 50€. Validators will then re-evaluate the evidence, utilizing the same adjudication process as the initial claim, to determine whether to lift the marker.

### 2.4 Recovery Protocol

*Initiating Recovery:* Once a claim is validated, the only way to remove the marker either is to transfer the funds to a specified GuardianChain smart contract wallet, or to submit a counter-claim.

*Fee and Redistribution:* The smart contract deducts a 1% fee on the recovered funds (used to repurchase GuardTokens and maintain token value) and then orchestrates the return of the remaining funds to the victim's original accounts, from where the funds were originally stolen. The repurchased tokens are locked in a smart contract and gradually air-dropped to users in the ecosystem, based on their involvement and participation, including to developers maintaining the GuardianChain blockchain.

## **3. Security and Privacy Considerations**

*Immutable Markers:* Once a marker is associated with a transaction, it becomes immutable. This ensures that marked funds remain identifiable until recovery.

*Validator Integrity:* The staking mechanism discourages malicious behavior by imposing financial penalties for any discrepancies in validation.

27<sup>th</sup> of September 2023

*Privacy:* The markers will integrate privacy-enhancing technologies such as zero-knowledge proofs to protect the data of those marking transactions, to avoid publicly disclosing the stolen funds' amounts or expose their transaction history, all the while retaining the transparency of the validation process.

#### **4. Future Work and Improvements**

*Scalability:* As adoption grows, the GuardianChain must ensure its capability to handle an increasing number of markers and validations.

*Interoperability:* Engaging with other public blockchains to standardize the marker recognition process will be essential.

*Privacy:* Ensuring the privacy of victims while maintaining transparency in the validation process needs careful balance.

*Integration with Traditional Authorities:* GuardianChain offers seamless integration capabilities with established law enforcement bodies, enabling them to utilize validated claims for pursuing potential culprits.

#### **5. Conclusion**

GuardianChain seeks to infuse trust and assurance into the crypto community. Through its decentralized, transparent, and community-driven initiative, it aims to minimize theft and offer a reliable recourse for victims without relying on centralized systems.

Adopting a system of public markers makes it easy for all actors within the blockchain space to integrate into their own blockchain projects, and include proportional measures that limit what can be done with marked funds until the suspicion is lifted or confirmed, without harming the user who is suspected of theft.

For more information:

Contact Martin Schmalzried: [www.martinschmalzried.com](http://www.martinschmalzried.com)