1inch Security

June 2024

ABSTRACT

1inch Security combines tools and technologies that 1inch has tested over the years. Many of them have been bundled into a SaaS offering called 1inch Shield API, available through the 1inch Developer Portal [https://1inch.dev/], to create a defensible line against bad actors in the decentralized finance (DeFi) space.

INTRODUCTION

DeFi boasts numerous benefits, including self-custody of funds; the ability to transact 24/7 with counterparties around the globe; the absence of intermediaries; and an emphasis on user privacy. However, these benefits can also be used by bad actors to conceal illicit activity, including digital asset theft, money laundering, concealing ill-gotten funds and defrauding legitimate participants in the DeFi ecosystem.

Traditional methods of preventing such bad acts, such as customer identification programs, transaction monitoring and other anti-money laundering ("AML") measures, are inapplicable to DeFi because funds are not held by a centralized entity, users do not create accounts, and there is no centralized actor that can pause a transaction before a smart contract executes it.

However, the public nature of on-chain activity means that DeFi projects can investigate and report illicit activity to law enforcement authorities and, in some cases, even prevent users from interacting with bad actors.

To protect users and make DeFi inhospitable to illicit actors, 1inch employs a mix of Web3 blockchain analytics and security services, Web2 detection and takedown services, optional user account creation services and suspicious activity reporting services. We constantly evaluate and assess the multitude of solutions we use as new technology becomes available.

1inch Security is the culmination of these efforts.

- 1inch internal blocklist program that includes behavioral patterns analysis and cybercrime intelligence
- Address screening and attributions by TRM Labs that include risk mitigators for downtime repercussions
- Address screening and labeling by Etherscan
- Transaction simulation and verification, token security and URL screening by Blockaid
- Scam website and profile detection and takedown by Phishfort
- Domain abuse and counterfeiting detection and takedown by Red Points
- Transaction simulation and verification, token security and URL screening by Blowfish for avoidance of downtime repercussions (coming soon)
- Device Intelligence (coming soon)
- 1inch Profiles and 1inch Pass (coming soon)
- Compliance AI agents (coming soon)
- Automated reporting (coming soon)

In the following sections, we will describe how 1inch uses or plans to use each of these services.

I. Address Screening

1. 1inch Blocklist Program

1inch has developed a comprehensive blocklist solution designed to ensure a safer and more secure DeFi ecosystem for legitimate users. This solution leverages multiple layers of investigation, community collaboration and direct partnerships with law enforcement agencies to address growing concerns about illicit activities taking place on blockchains.

(a) Internal Blockchain Investigation Back Office

At the core of 1inch's blocklist program is the internal blockchain investigation back office. This team is responsible for:

- Monitoring Transactions: The team continuously monitors blockchain transactions to identify suspicious activities.

- Analyzing Data: Using advanced analytics and forensic tools, the team analyzes transaction patterns to detect potential illicit activities, such as money laundering, fraud or funding illegal operations.

- Behavior-based blockchain risk monitoring. Screening tools can flag risk based solely on the activity of a given address (i.e., whether the given account is engaging in unusual behavior or actions typical of somebody laundering money).

- Creating a Blocklist: Based on its findings, the team compiles blocklists of addresses involved in suspicious or confirmed illegal activities.

(b) Community of Investigators

The wider crypto community plays a crucial role in maintaining the integrity of the blocklist:

- Crowdsourced Intelligence: Thanks to blockchain's inherent transaction transparency, a remarkable and truly decentralized community of blockchain enthusiasts has developed over the years, identifying and reporting suspicious activities to public sources. 1inch leverages their contributions as an early warning system, which our internal team investigates, confirms and, if merited, adds to the 1inch blocklist.

- Responsive Action: When suspicious activities are reported, the community reacts swiftly to verify and take necessary actions. This ensures that the blocklist is constantly updated and reflects the latest intelligence.

(c) Direct Collaboration with Law Enforcement Agencies

1inch works closely with law enforcement agencies to enhance its blocklist solution:

- Source of Intelligence: Law enforcement agencies provide us direct and vital information on addresses and activities linked to illicit activities. This helps 1inch to stay ahead in identifying and blocking such addresses.

- Preventive Measures: Through these collaborative efforts, 1inch can take proactive steps to prevent the use of its platform for illegal activities.

(d) Integration with Public Lists

The 1inch blocklist integrates publicly available lists from reputable sources to enhance its effectiveness:

- Circle and Tether: These organizations publish lists of banned addresses that have been identified as involved in illegal activities. 1inch's blocklist incorporates these lists to ensure comprehensive coverage.

- Dune Queries: Utilizing Dune Analytics, 1inch can query and cross-reference public data sets for additional banned addresses. This helps validate internal findings and ensure alignment with the broader blockchain community's efforts.

(e) Cybercrime Intelligence Solution

1inch integrates decisive threat intelligence to reduce risk and increase protection by collaborating with leading cyber intelligence vendors that provide comprehensive data and insights on cyber threats, enabling proactive measures against potential risks.

- Enhanced Protection: By integrating intelligence from these vendors, 1inch can identify and respond to emerging threats more effectively, ensuring higher levels of security.
- Reduced Risk: This collaboration allows 1inch to preemptively block interactions with high-risk entities.

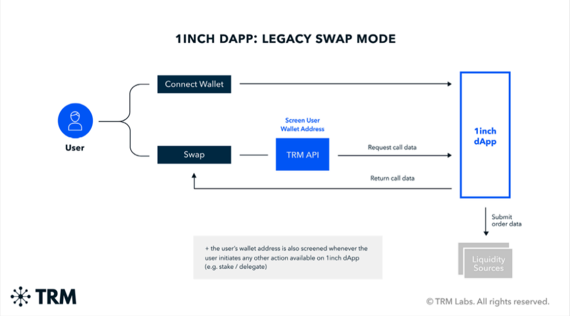
This multi-layered approach not only enhances the security of 1inch's platform but also contributes to the broader goal of making the DeFi ecosystem safer for all participants, especially through 1inch API offerings.

2. TRM Labs

Identifying and blocking potential bad actors based upon a range of risk categories, including sanctions, fraud, darknet markets exposure and other indicators of financial crime, is a top priority for 1inch. Since 2022, 1inch has used TRM Labs' on-chain crypto fraud and financial crime detection tool to screen user wallets.

Using TRM's API, 1inch queries data about addresses and transactions, including on-chain exposure to sanctions, terrorist financing, hacked or stolen funds, hacker groups, ransomware, scams, human trafficking and child sexual abuse material. Using a list created from hundreds of millions of sources, TRM's API subsequently returns a risk score that indicates if the address (a) is owned, controlled, or associated with a sanctioned entity or other form of illegal activity (ownership risk) or (b) has transacted with a sanctioned address or one associated with illegal activity (counterparty risk).

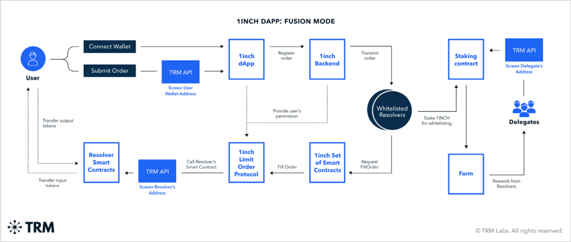
1inch automatically restricts users that come up with certain risk factors, preventing them from connecting to the 1inch dApp, 1inch Wallet or 1inch's APIs, as well as from conducting any transactions via these services (e.g., staking or delegating). Users can request a manual review if they believe they have been misclassified.


1INCH DAPP: LEGACY SWAP MODE

+ the user's wallet address is also screened whenever the user initiates any other action available on 1inch dApp (e.g. stake / delegate)

© TRM Labs. All rights reserved.

In 1inch's Fusion mode, third party resolvers or professional market makers (PMMs) execute gasless swap transactions. Each third party that wishes to provide such services must pass identity verification and a wallet screening by TRM before 1inch whitelists them as a resolver or PMM. Wallet screening then continues as part of every settlement performed by these third parties.


1INCH DAPP: FUSION MODE

© TRM Labs. All rights reserved.

3. Etherscan Pro

Blockchain analytics focuses on linking pseudonymous data (assets, addresses, events) to real-work people, entities and events. Attribution methods and sources vary. Because so many swap transactions take place on Ethereum, 1inch employs Etherscan Pro, in addition to TRM Labs, for screening purposes.

Etherscan API Pro provides additional endpoints and higher rate limits for subscribers. 1inch leverages Etherscan's breadth, depth and speed of labeling to amplify the efficacy of our screening efforts.

When a wallet connects to the 1inch interface, 1inch sends simultaneous requests to TRM Labs and Etherscan. The wallet remains inactive and unable to transact until a positive answer is returned.

4. Cross-chain Security (coming soon)

Vulnerabilities in cross-chain bridges make cross-chain security a key part of any DeFi security strategy, especially the capability to conduct and visualize multi-asset, cross-chain investigations in a single graph. 1inch is working on technological solutions as well as expanding our investigative abilities in this key area.

5. Behavioral pattern analysis (coming soon)

Behavioral risk detection capabilities empower 1inch to uncover suspicious activity, even in cases where linking an address to an entity is impossible. Advances in machine learning allow investigators to search for on-chain patterns in the way funds move and uncover additional wallets involved. 1inch is studying options to incorporate these innovations into our security strategy.

6. Downtime Risk Mitigation (coming soon)

Systems are only as good as their backups. To mitigate the risks of screening service outages or downtime, 1inch is considering and assessing alternative and/or additional screening solutions.

II. Front-end User Protection

While address screening helps to prevent wallets associated with illicit activity from accessing the 1inch platform, such tools as transaction simulation and validation help users recognize potential issues with a transaction, dApp or token they intend to interact with, functioning as the Web3 equivalent of antivirus software.

1. Blockaid

1inch's self-custody wallet offers users a convenient way to access 1inch and other DeFi platforms on their phones. 1inch uses multiple Blockaid APIs to help protect wallet users: dApp scanning, transaction simulation and validation, as well as malicious token detection.

(a) dApp Scanning

1inch Wallet users receive protection from malicious dApps through Blockaid's dApp Scanning API, which finds and scans malicious dApps and alerts the user before connecting to a website that might be malicious. 1inch Wallet users also benefit from the identification of messages that contain malicious domains, akin to email services flagging spam for their users.

(b) Transaction Simulation and Validation

Transaction simulations help 1inch Wallet users understand exactly what will happen when they sign a transaction, i.e., what functions will be executed by the smart contract and what the user is allowing the smart contract to do in their 1inch Wallet. Users receive alerts indicating which assets will be withdrawn from their 1inch Wallet and which assets will be deposited. In the validation process, the transaction is subsequently assessed and categorized as malicious or benign. The simulation and validation results are displayed as warnings in the user interface when threats are detected.

(c) Malicious Token Detection

1inch Wallet users also benefit from Blockaid's Malicious Token Detection API, which distinguishes between spam and legitimate tokens. Spam tokens are automatically hidden from the user, while suspicious ones are flagged.

2. Blowfish (coming soon)

1inch employs a similar approach to front-end warning systems as it does with wallet screening. As methods and sources vary, 1inch engages two leading companies to provide transaction simulations and dApp screenings to mitigate downtime repercussions and potentially prevent extra risks. 1inch Wallet users receive a warning before engaging with harmful dApps and before signing a potentially malicious transaction.

III. Brand Abuse Takedowns

At first glance, brand protection might not appear to be a security tool. But as 1inch has grown, the number of fraudsters exploiting the 1inch name to scam users and steal their funds has also increased.

Many types of brand abuse fraud schemes exist, including impersonation websites that incorporate 1inch's name and fake social media accounts used by scammers to steal users' funds. Another scam involves the scammer persuading the user to conduct a transaction through the 1inch platform, but the user's funds are diverted to the scammer's wallet. Many DeFi scams happen in direct messages and involve the scammer requesting an advance payment for something that is never sent.

1. Phishfort

1inch works with Phishfort to combat phishing, fake content and IP infringements. While Phishfort scans the web for brand threats, the 1inch support team and other contributors also actively report scammers and fraudsters to Phishfort to facilitate their removal.

2. Red Points

1inch works with Red Points to identify and take down fake websites, social media accounts and apps. Red Points' AI-based searching algorithm performs automatic sweeps to detect 1inch impersonations.

1inch is able to track alerts and infringements, as well as enforcement status, through its Red Points dashboard.

IV. Optional User Authentication

1. 1inch AI Agent (coming soon)

The intersection of AI and blockchain comprises a wealth of opportunities to harness the power of machine learning and AI for preventing illicit activity and protecting crypto users. This solution integrates advanced AI technology within an operating system to create a personal AI assistant that prioritizes user privacy and security.

(a) Personal AI Assistant

At the heart of the 1inch AI agent solution is a personal AI assistant driven by four guiding principles:

- User-owned: The AI agent solution introduces the concept of "user-owned AI." The AI agent is integrated into the user's wallet, providing constant oversight and protection for the user, like a personal bodyguard.

- Protection: The AI assistant helps users avoid interactions with organized crime or scammer dApps, ensuring a safer DeFi experience. The AI assistant is always on guard, monitoring transactions and interactions to detect and stop any suspicious or harmful activities.

- Personalization: The AI assistant is tailored to a user's specific needs, providing highly optimized and personalized assistance that improves with each transaction.

- Privacy: The AI assistant prioritizes privacy and operates without disclosing users' private information or assets.

(b) Privacy-First Trust Framework

The AI agent solution addresses a persistent dilemma in the DeFi space: balancing users' right to privacy with preventing illicit activity and protecting users and the ecosystem from bad actors. Without adequate safeguards, the growth and maturation of DeFi markets are hindered. But AI assistants can protect privacy while also providing safeguards through:

- Risk Assessment: Each AI assistant continuously assesses its user's risk based on interactions and transaction history.
- Transparent Sharing: When required, and with the user's consent, the AI assistant can share its user's risk score with financial intermediaries or dApps, providing an additional layer of transparency and security in the DeFi ecosystem.
- Enhancing Trust: By implementing an objective risk scoring system, the AI agent helps build trust between users and financial platforms, facilitating smoother and more secure transactions.

(c) Peer-to-Peer AI Interactions

The AI assistant can easily interact and transact with wallets that do not have AI agents integrated. Over time, however, we envision AI-to-AI interactions becoming commonplace within the community, enabling the following:

- Seamless Transactions: Users' AI assistants can engage in peer-to-peer transactions, facilitating seamless and secure interactions without exposing personal data.
- Collaborative Community: This system fosters a community of AI agents that collaborate to enhance the overall security and efficiency of the DeFi ecosystem.

1inch's planned AI agent solution will represent a significant advancement in ensuring user safety and optimizing interactions within the DeFi ecosystem. Its innovative approach combines privacy, security, and community collaboration to provide a comprehensive and user-friendly experience.

2. 1inch Profiles and 1inch Pass (coming soon)

1inch will soon offer users a new product called 1inch Profiles, intended to serve as an enhanced security, transparency and education resource for users, with an added functionality for a more streamlined and familiar experience. 1inch Profiles will be complemented with an identification and verification tool: 1inch Pass.

(a) 1inch Profiles Account Functionality

1inch Profiles are users' functional accounts enabling them to keep track of their wallets, registered devices and sessions, as well as transactions. Log-ins through social accounts and passkeys will be enabled. 1inch Profiles also offer easy access to other 1inch products, such as the 1inch Portfolio.

(b) 1inch Pass

1inch Pass is an entry point for the Know-Your-Customer (KYC) process: user identification and wallet screening. 1inch Pass comes as a mobile application, a gateway for the user's securityg. An SDK, returning proof of verification, will be offered as a solution to other dApps, looking to bring security into the DeFi space.

(c) DeFi Education

In addition to improving 1inch user experience, we view 1inch Profiles as an entertaining gateway resource informing users about the unique aspects of DeFi and self-custody solutions, especially the risks inherent to the ecosystem and available mitigators for such risks (which are numerous, but are rarely adopted by users).

- 1inch Profiles users can choose to interact with educational materials as a non-linear, choose-your-own-adventure style journey, based on the user's pre-existing knowledge. Users can intuitively navigate, for instance, from risk disclosures to a glossary of associated terms, Users can gradually build a comprehensive knowledge base on risks and prevention practices before exploring a library of proposed tools.

- Games and quizzes provide the user with opportunities to test themselves, including an appropriateness test that assesses the user's knowledge and skills in DeFi interactions and makes suggestions for improvement.

- Users will have a chance to win rewards and other incentives by engaging with the resource.

- 1inch Profiles features a reputational scoring system that, apart from assessing on-chain behavior with 1inch Security tools, will also assess user engagement with educational resources, gamifying the experience.

The scope of educational materials ranges from general risks associated with blockchain and virtual currencies to the benefits of smart accounts for fund management. Possible topics include:

- How to prevent exposure to illicit activity, scams, attacks and other vulnerabilities through the tools included in 1inch Security, and an in-depth explanation of the library of tools that users can implement on an individual or small scale level for all their DeFi interactions.

- How user security is enhanced through 1inch dApp solutions' inherent functionalities, like MEV protection, gasless swap execution, intent-based architecture and price impact protection offered by 1inch Fusion.

- Strategies to increase resilience to self-custody risks, including methods to prevent loss of access to wallets and funds, through smart account solutions available on the market. These smart accounts enable additional and more familiar behavior for the user, including social sign-ins, use of passkeys for log-ins and signing transactions and social recovery based on trusted devices or accounts.

- How the user's trading experience may be streamlined through smart accounts and accounts abstraction, which enable the user to set transaction limits, use temporary session keys and set up role-based permissions for corporate accounts.

The wide variety of disclosed risks are intended to alert the user, immediately providing them with solutions applicable to the entire ecosystem.

V. Device Intelligence (coming soon)

1inch will soon engage a provider of device intelligence and behavioral signals to amplify our investigation capabilities. The presence or likely presence of bots, emulators, true IP mismatches, time zone mismatches, OS anomalies, remote software and other factors is assessed and combined into a resulting device reputation rating. Combined with blockchain intelligence, this reputation rating will assist 1inch in determining the likelihood of illicit activities.

1inch is one of the first DeFi projects to partner with a provider of device intelligence tools to enhance investigation efforts.

VI. Automated Reporting (coming soon)

1inch supports law enforcement agencies' efforts across the globe to investigate criminal activity and responds to all legitimate law enforcement requests for information (within the boundaries of applicable data protection laws and regulations).

Suspicious Activity Reports play a critical role in alerting law enforcement agencies to potential instances of money laundering and other illicit activity. We explored the possibility of submitting SARs to financial intelligence units but quickly realized that SAR filings required information unavailable in the permissionless space. We subsequently opened a dialogue with select financial intelligence units and law enforcement agencies to ascertain how 1inch could proactively assist them in fighting crime. Ideas include building an automated reporting function that would supply these agencies with information of interest before data retention periods expire and prior to the potential degradation of the evidentiary trail.

CONCLUSION

1inch Security represents 1inch's ongoing efforts to prevent bad actors from exploiting the platform and to protect users from scams, hacks, and fraud. As regulatory and legislative efforts lag behind technological advances, market leaders like 1inch must proactively assess and implement measures to guide DeFi towards a safer and more secure future.