Rooted

Rooted is a non-custodial solution that uses stealth addresses which will allow users to receive funds on Rootstock Blockchain without revealing receivers real address.

Project Description

Project Overview

- Rooted is a privacy-focused solution addressing the need for anonymity in blockchain transactions. It tackles the risk of exposing the identities and financial information of users by enabling anonymous transactions on the Rootstock Blockchain. The solution utilizes stealth addresses on the Rootstock Blockchain, allowing users to receive funds without revealing their real addresses.
- The project draws inspiration from existing privacy-focused blockchains like Monero and tools like Tornado Cash, but aims to bridge the gap between complex and expensive privacy solutions and non-private transfers.
- It empowers users to maintain their privacy, fostering trust and security in the blockchain industry.
- Overall, Rooted has the potential to become a leading privacy solution, ensuring the confidentiality and anonymity of blockchain transactions.

Idea

- I've always been fascinated by the concept of anonymity in blockchains, with various methods available to achieve it.
- Privacy-focused blockchains like Monero and widely-used networks like Tornado Cash, which is based on anonymity sets or zero-knowledge proof solutions, provide near-perfect privacy for both parties in a transaction.
- However, they require specialized tools or come at a higher cost than direct transfers, leaving a gap between expensive, complex solutions and non-private transfers.
- Recently, Vitalik published an article titled "An Incomplete Guide to Stealth Addresses," which provided missing pieces of a simple yet effective solution for anonymous transactions, at least for the receiving party.
- Inspired by this idea we decided to create a user-friendly tool utilizing stealth addresses. We chose Rootstock as the initial network for its implementation due to its fast and affordable transactions.
- The name Rooted is chosen as users will be rooted in such a way that they will become anonymous while doing transactions.

Background & Context

- The problem that Rooted is tackling is the lack of privacy in blockchain transactions. While blockchain technology offers transparency and immutability, it also exposes transaction details, including sender and receiver addresses. This lack of privacy poses risks for individuals and businesses, as their financial activities can be tracked and potentially linked to their real-world identities.

- Privacy is a fundamental aspect of financial transactions. Without privacy, users are susceptible to various risks, including:

    - **Identity exposure:** When transactions are conducted openly on a blockchain, it becomes possible for observers to connect transactions with specific individuals or businesses. This can lead to the loss of financial privacy and potential targeting or surveillance.

    - **Financial profiling:** Analyzing blockchain transactions can enable third parties to build detailed profiles of individuals and businesses, including their spending habits, income, and financial relationships. This information can be used for targeted advertising, discrimination, or even extortion.

    - **Security vulnerabilities:** Repeatedly using the same address for receiving funds on a transparent blockchain can make users vulnerable to hacking or phishing attacks. Attackers can analyze transaction history to identify patterns, monitor account balances, and exploit weaknesses in security.

    - **Business competition:** Companies conducting transparent transactions may inadvertently reveal sensitive financial information, such as sales volume, supply chain relationships, or partnerships. Competitors could exploit this information for their advantage, compromising the competitiveness of businesses.

    - **Compliance concerns:** Certain industries, such as healthcare or finance, require strict privacy regulations. Transparent blockchain transactions may conflict with these regulations, leading to legal issues or non-compliance penalties.

- The importance of tackling this problem lies in the preservation of financial privacy and the protection of individuals' and businesses' sensitive information. By offering a user-friendly solution for anonymous transactions through stealth addresses, Rooted aims to empower users with greater control over their financial privacy and mitigate the risks associated with identity exposure.

Value Proposition

- **Enhanced Privacy:** Rooted utilizes stealth addresses, allowing users to receive funds without revealing their real addresses. This provides a significant level of

privacy for individuals and businesses, ensuring that their financial activities are shielded from prying eyes.

- **User-Friendly Solution:** Rooted aims to be accessible and user-friendly for both power users and non-power users. The generation and usage of Rooted IDs and stealth addresses are designed to be simple and intuitive, enabling a wide range of users to adopt and utilize the solution without technical complexity.

- **Affordability and Speed:** Rooted is built on the Rootstock Blockchain, chosen for its fast and affordable transactions. By leveraging this blockchain, Rooted offers users the benefits of privacy without sacrificing transaction speed or incurring high fees commonly associated with other privacy-focused solutions.

- **Bridge the Gap:** Rooted fills the gap between expensive and complex privacy solutions, such as Monero, and non-private transfers on transparent blockchains. It provides an intermediate solution that offers a significant level of privacy without the need for specialized tools or high costs.

- **Wide Applicability:** Rooted's privacy solution can be applied to various use cases. It can benefit individuals who want to keep their financial transactions private, businesses that need to protect their financial information, and anyone concerned about the risks associated with revealing their identity during transactions.

- **Market Differentiation:** Rooted stands out in the market by offering a unique approach to privacy in blockchain transactions. While other solutions rely on heavy computations or complex methodologies, Rooted simplifies the process with stealth addresses and Rooted IDs, making it more accessible and user-friendly.

What it will do or Technical Description

- **Stealth Addresses:** Rooted utilizes stealth addresses, which are derived from elliptic curve key pairs. The public part of the key pair serves as the Rooted ID, a meta-address not tied to any actual blockchain address. This Rooted ID is shared by users to receive funds without revealing their real addresses.

- **Rooted ID Generation:** Users can generate multiple Rooted IDs, storing the key for future use. This allows them to have different Rooted IDs for different transactions or purposes, enhancing privacy. The generation process follows the principles outlined in Vitalik's article on stealth addresses.

- **Transaction Process:** When a user wants to send funds to a recipient, the sender calculates a stealth address using the recipient's Rooted ID and an ephemeral private key. This creates a new and unpredictable stealth address for each transfer. The sender then initiates a transaction to the Registry contract on the Rootstock Blockchain.

- **Registry Contract:** The Registry contract is an essential component of Rooted. It facilitates the transfer of funds to stealth addresses. The sender includes their ephemeral public key in the transaction, and the contract handles the transfer of funds to the calculated stealth address.

- **Receiver Monitoring:** The recipient, using their Rooted ID's private part, monitors the Registry contract for new keys published by senders. They attempt to construct a private key and corresponding stealth address using their Rooted ID. If the derived stealth address contains funds, it indicates that it is the stealth address where the funds were sent.

- **Funds Withdrawal:** Once the recipient identifies the stealth address with funds, they obtain the corresponding private key. This key can be used in any wallet software or to transfer funds directly from the Rooted website to another party, exchange, or cold wallet. By not withdrawing funds to a personal address, the connection between the recipient and sender remains hidden.

- **RIF Technologies:** Rooted leverages the capabilities of the Rootstock Infrastructure Framework (RIF) technologies. This includes the use of the Rootstock Blockchain, which offers fast and affordable transactions suitable for implementing the privacy features of Rooted.

- **Addressing Privacy Concerns:** Rooted addresses the problem of privacy in blockchain transactions by providing a user-friendly solution that allows individuals and businesses to receive funds without revealing their real addresses. By utilizing stealth addresses and Rooted IDs, Rooted ensures that transaction details remain private and reduces the risk of identity exposure and financial profiling.

Intended Users

- The intended users of Rooted would be anyone who values privacy in their transactions and wants to keep their identity hidden. This could include individuals who want to keep their financial transactions private, businesses that want to protect their financial information, or anyone who wants to avoid the risks associated with revealing their identity in a transaction.
- Rooted will be designed to be user-friendly for both power and non-power users, making it accessible to a wide range of people.

Market Analysis

- Rooted's solution addresses a significant market opportunity by providing privacy in blockchain transactions. Privacy has become a crucial concern in the blockchain industry as individuals and businesses increasingly recognize the risks associated with transparent transactions. By offering a user-friendly and accessible solution, Rooted taps into a growing demand for privacy-enhancing tools in the blockchain space.

- The Total Addressable Market (TAM) for Rooted's solution is substantial. As blockchain technology continues to gain adoption across industries, the need for privacy in transactions becomes more prevalent. Individuals who value financial privacy, businesses seeking to protect sensitive financial information, and anyone concerned about the risks of identity exposure in transactions represent a wide range of potential users for Rooted.
- Rooted differentiates itself from incumbent competitors by providing a simpler and more cost-effective solution. Existing privacy-focused blockchains like Monero require specialized tools and incur higher costs, making them less accessible to mainstream users. Rooted bridges the gap between complex and expensive privacy solutions and non-private transfers, offering a user-friendly option with its stealth address implementation. The ease of generating Rooted IDs and utilizing stealth addresses sets Rooted apart from incumbent competitors.
- Furthermore, Rooted leverages the Rootstock Blockchain, which provides fast and affordable transactions. This strategic choice enhances the scalability and usability of the solution, making it attractive to users who prioritize transaction speed and cost-efficiency.

Project Plan

- **Development and Testing:** The first step is to develop the Rooted solution and the necessary smart contracts on the Rootstock Blockchain. The development team will use tools like Solidity and Hardhat to build and test the functionality of Rooted, ensuring its effectiveness and security.

- **UI/UX Design:** Simultaneously, a user-friendly and intuitive UI/UX will be designed using technologies such as React and TypeScript. The focus will be on creating a seamless and engaging experience for both power users and non-power users, making it accessible to a wider audience.

- **Alpha and Beta Testing:** The developed solution will undergo rigorous testing in alpha and beta phases. This includes testing the functionality, performance, and security aspects of Rooted. Feedback from users and testers will be invaluable in refining the solution and improving the overall user experience.

- **Launch and Marketing Strategy:** Once the Rooted solution is stable and polished, it will be officially launched to the market. A comprehensive marketing strategy will be implemented to create awareness and attract users. This may include content marketing, social media campaigns, partnerships with relevant blockchain communities, and targeted advertising.

- **User Education and Support:** Alongside the launch, user education and support will be provided to ensure users understand the benefits of Rooted and how to utilize it effectively. This can be done through tutorials, documentation, FAQs, and a responsive support system. Engaging with the community and addressing user concerns will be crucial to building trust and loyalty.

- **Partnerships and Integrations:** To expand the reach and adoption of Rooted, strategic partnerships can be established with exchanges, wallets, and other

blockchain platforms. Integration with popular wallets and exchanges will make it convenient for users to transact privately using Rooted. Collaborations with other privacy-focused projects or organizations can also help in creating a strong network effect.

- **Continuous Improvement and Updates:** Rooted will undergo continuous improvement based on user feedback, market trends, and advancements in blockchain technology. Regular updates and feature enhancements will be rolled out to ensure that Rooted remains competitive and aligned with user needs.

- **Compliance and Regulations:** Rooted will comply with relevant regulations and ensure that it adheres to legal frameworks. This includes addressing any concerns related to privacy regulations and working towards compliance in different jurisdictions.

By following this plan, Rooted aims to build a strong presence in the market, attract a significant user base, and become a trusted and widely adopted solution for privacy in blockchain transactions.

Challenges

- The main challenge we believe will be designing the best possible user experience, as for mass adoption it should be as simple as it can be to use.

Team and Resources

- **Team Members:**

  - Shubham Gupta: Full-Stack Blockchain Developer with a strong knack for Entrepreneurship. Shubham will bring technical expertise and leadership to the development and implementation of Rooted.
  - Twitter Id: https://twitter.com/0xmysticShub

- **Team-Market Fit:**

  - The team is well-positioned to tackle the market opportunity presented by Rooted. With a strong background in blockchain development and a focus on entrepreneurship, Shubham Gupta understands the technical intricacies of building privacy solutions and possesses the necessary skills to navigate the market and drive adoption. This team-market fit ensures that the project can be executed effectively and aligns the team's expertise with the demands of the target market.

- **Resources Required:**

  - Technical Resources: Solidity and Hardhat will be utilized for smart contract development. React and TypeScript will be used for UI/UX development.

These resources will enable the team to build the Rooted solution and create an intuitive user interface.

- ✧ Rootstock Blockchain: Rooted will leverage the Rootstock Blockchain for its fast and affordable transactions. The features and capabilities of the Rootstock Blockchain will be utilized to implement the privacy-enhancing functionalities of Rooted.
- ✧ Development Tools: Tools such as IDEs (Integrated Development Environments), code editors, version control systems (e.g., Git), and testing frameworks will be utilized to streamline the development and testing processes.
- ✧ Marketing and Communication Resources: Resources will be allocated to marketing efforts, including content creation, social media management, community engagement, and advertising. These resources will help create awareness about Rooted and effectively communicate its value proposition to the target audience.
- ✧ Partnerships and Collaborations: Strategic partnerships and collaborations will be pursued to enhance the reach and adoption of Rooted. This may involve collaborating with exchanges, wallets, and other blockchain platforms to integrate Rooted's functionality and expand its user base.
- ✧ User Support and Education: Resources will be allocated to providing user support and education, including documentation, tutorials, FAQs, and a responsive support system. These resources will ensure that users have the necessary guidance to understand and utilize Rooted effectively.
- ✧ Compliance and Legal Resources: Resources will be allocated to ensure compliance with relevant regulations and legal frameworks. This may involve legal counsel and compliance experts to address any privacy-related concerns and navigate the regulatory landscape.

Conclusion

- ➢ Rooted is a user-friendly and innovative solution that addresses the growing need for privacy in blockchain transactions. By leveraging stealth addresses and the Rootstock Blockchain, Rooted provides a simple and cost-effective way for users to keep their financial transactions private. With a substantial market opportunity and a focus on usability, Rooted has the potential to become a leading privacy solution in the blockchain industry.