Shielded Accounts: *A Vanguard Approach to Privacy in DeFi Transactions*

w36d

Redacted Labs

***Abstract* — With the continuous growth and acceptance of the DeFi sector, user privacy becomes an area of increasing concern. Blockchain technology offers transparency and security but often falls short in providing the necessary transactional privacy[7,8,9]. Shielded Accounts propose a solution by leveraging zk-SNARK technology[1,2,3,4,5] to ensure that while transactions are verifiable, specific transactional details remain confidential, preserving user privacy.**

I. Introduction

Blockchain technology's inherent transparency, while a boon for public verifiability, has unfortunately exposed all transactional information to the public eye[7,8,9]. This means that, for most blockchains, anyone with a public address can view all associated transactions, including the value transferred and the addresses involved[7,8,9]. As a result, blockchain users can potentially be targeted by malicious parties who have access to their transactional information. Shielded Accounts, proposed herein, offer an essential solution to this problem.

II. Background

A vast majority of blockchain platforms, such as Bitcoin and Ethereum, offer no inherent privacy mechanism, exposing all transactional information publicly[7,8,9]. Some privacy-focused chains like Monero and Zcash have sought to address this issue, but their solutions often involve the entire blockchain, limiting interoperability with other chains[2]. In contrast, Shielded Accounts allow for transactional privacy at an account level, enabling privacy on demand and broad compatibility across different chains.

III. Shielded Accounts

Shielded Accounts leverage zk-SNARKs technology, a type of zero-knowledge proof that allows one party to prove possession of certain information without revealing it[4,5]. In the context of blockchain transactions, this means that a user can prove that they have a valid transaction without revealing the specific details of that transaction, such as the sender, receiver, and value transferred. This not only protects the user's privacy but also ensures that the transaction is valid and free from doublespending[1,2,3,4,5].

IV. Technical Architecture

The Shielded Accounts system is built around a technical architecture that combines the robustness of smart contracts with the privacy capabilities of zero-knowledge proofs. It comprises two fundamental components:

A. Proxy Smart Contract

At the heart of the Shielded Accounts system is the Proxy Smart Contract. This contract acts as an intermediary between the user and the DeFi ecosystem and is deployed directly on the blockchain. When a user wishes to initialize a Shielded Account, they deposit tokens into the Proxy Smart Contract. Upon receipt of this deposit, the contract records a hash of the depositor's public address, effectively creating a private, on-chain account for the user. It is important to note that this process does not expose the user's private account details. The Proxy Smart Contract plays a critical role in ensuring the privacy of transactions. When a user wishes to execute a trade or provide liquidity, they interact with the contract, which processes the request in a way that preserves the privacy of the user's account. All transactions are executed within the contract, maintaining privacy and ensuring proper execution.

B. zk-SNARKs

The Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) mechanism represents a sophisticated cryptographic architecture, whose chief role is to facilitate transactions that inherently uphold the principles of privacy.

When the context revolves around the construct of Shielded Accounts, zk-SNARKs act as a powerful tool, permitting participants to convincingly affirm the possession of certain data elements without necessitating the exposure of the data in question.

When a participant intends to carry out a transaction, an off-chain zk-SNARK proof pertinent to the transaction is synthesized. This cryptographic proof, serving as an encoded analogue of the transaction, is forwarded to the Proxy Smart Contract. Subsequently, the Proxy Smart Contract holds the ability to validate the integrity of the transaction, all the while maintaining ignorance of the transaction's specific details - this preserves the user's privacy in an uncompromised manner.

Consider a zk-SNARK proof, denoted by the symbol π, related to a particular statement, symbolized by x, and a witness, symbolized by w. The computation of π adheres to the following protocol:

$$\pi = \textit{zk-SNARK\_Prove}(x, w)$$

To ascertain the validity of the proof, the zk-SNARK_Verify function comes into play. This function accepts the statement, x, and the proof, π, and generates a boolean value that signifies the authenticity of the proof:

$$\textit{isValid} = \textit{zk-SNARK\_Verify}(x, \pi)$$

Hence, the zk-SNARKs protocol provides a robust, privacy-centric framework, equipped to verify transactional integrity without the need to disclose any sensitive or specific data.

V. Transaction Execution

The process of executing a transaction within a Shielded Account is designed to ensure privacy and correctness.

When a user wishes to execute a transaction (e.g., a token swap or liquidity provision), they first generate a zk-SNARK proof for the transaction off-chain. They then submit this proof, along with encrypted transaction details, to the Proxy Smart Contract.

Upon receipt of the proof and encrypted transaction details, the Proxy Smart Contract first verifies the validity of the proof. If the proof is valid, the contract then executes the transaction with the DeFi platform.

The resulting tokens from the transaction are credited to the user's Shielded Account within the Proxy Smart Contract. At no point during this process are the user's private account details or specific tokens involved in the transaction exposed to the DeFi platform or to the public blockchain.

The user can withdraw their tokens back to their original deposit address at any time, preserving privacy while ensuring regulatory compliance.

VI. Privacy-Preserved Liquidity Provision and NFT Transactions

Beyond enabling privacy-preserving transactions, the Shielded Accounts infrastructure extends this capability to include provision of liquidity and Non-Fungible Token (NFT) transactions. These functionalities provide an elevated layer of privacy in actions that typically require revealing of public addresses or transaction data.

A. Liquidity Provision

Users intending to contribute to liquidity pools, usually have to submit their liquidity provider (LP) tokens, publicly. With the Shielded Accounts architecture, the process undergoes a notable transformation for enhanced privacy.

Users deposit their LP tokens into the Proxy Smart Contract. The contract assumes an acting role on behalf of the user, interacting with the liquidity pool in question. These interactions are processed off-chain through zk-SNARK proofs to preserve privacy. Hence, the actual movement of tokens related to liquidity provision is obscured from public view, creating an added layer of privacy.

Meanwhile, the user's interactions with the liquidity pool, such as adding or removing liquidity, are abstracted into zk-SNARK proofs. The Proxy Smart Contract then verifies these proofs and executes the interactions accordingly. Notably, the anonymity of the user is maintained, and the execution results of these actions are the only pieces of information recorded on-chain.

B. NFT Transactions

NFT transactions often necessitate the disclosure of ownership or transaction information. However, within the Shielded Accounts infrastructure, users can keep their interactions with NFTs private.

Similar to the liquidity provision process, users deposit their NFTs into the Proxy Smart Contract. The contract, serving as the acting entity, then communicates with the NFT marketplace. The user's interaction, such as buying, selling, or transferring NFTs, is processed off-chain and converted into zk-SNARK proofs.

The Proxy Smart Contract verifies these proofs, preserving the privacy of the user's NFT transactions. The contract executes the transactions, and only the outcomes of the transactions are recorded on-chain, thus effectively shielding the user's NFT transactions from public visibility.

With these functionalities, the Shielded Accounts infrastructure brings robust privacy solutions to an expanded range of activities in the DeFi space, contributing towards a secure, and privacy-conscious DeFi ecosystem.

VII. Regulatory Compliance

In a global environment that is increasingly emphasizing regulatory compliance and legal adherence, especially in the context of cryptocurrency transactions, privacy-focused solutions must align with the regulatory frameworks to foster wider acceptance[6]. A significant feature of Shielded Accounts is its alignment with these principles[6].

A cornerstone of the Shielded Accounts' design is that the withdrawal of funds can only occur to the originating address of the deposit. This allows for the tracking of asset flow from the perspective of the origin and final destination of the assets. This is crucial in maintaining transparency of fund ownership, a key tenet in various Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations.

While transactional privacy is maintained throughout the use of the Shielded Account, the starting and end points of the transaction flow are verifiable on the public blockchain. This inherent transparency provides a balance between user privacy and the necessary compliance with regulatory standards.

Redacted respects and upholds the autonomy and privacy of its users even while facilitating transparency. With that in mind, we've devised a system that allows users, at their discretion, to generate a read-only private key. This read-only key can be shared with i.e. auditors or tax consultants if the user chooses to do so, providing a means for them to examine transactions without compromising the actual control or privacy of the user's activities.

It is exclusively the user's choice to create and distribute this key, further ensuring user control and privacy. This unique feature balances the need for privacy with the potential requirements of compliance and auditability.

In essence, while transactions made via the Shielded Account are masked to the public, they are not entirely anonymous. The originating deposit address serves as a pseudo-identity within the system, allowing for the mapping of asset ownership. This feature is paramount, especially within jurisdictions that mandate transparency of digital asset ownership and flows.

It should be noted that while the Shielded Account structure has been designed to align with prevailing regulatory standards, users and platforms that employ this technology should seek independent legal advice pertinent to their jurisdiction. The legislative landscape around digital currencies and privacy is rapidly evolving, and it is crucial for stakeholders to keep abreast of the changing legal and regulatory requirements.

This design reflects a commitment to working within the existing regulatory frameworks while offering a viable solution for privacy-focused transactions in decentralized finance. The compliance feature does not impede the utility or effectiveness of the Shielded Accounts but instead encourages its wider adoption among entities that are required to abide by these regulations.

Please note, this document should not be regarded as legal advice. Individuals and entities are advised to consult with their legal counsel regarding regulatory compliance related to their specific circumstances.

VIII. User Experience

While privacy, security, and regulatory compliance are central to the design of Shielded Accounts, the user experience has not been overlooked. The system has been designed to be as seamless and straightforward as possible, allowing users to interact with the DeFi ecosystem without having to manage complicated privacy-preserving techniques themselves.

When a user wishes to initialize a Shielded Account, they simply deposit their tokens into the Proxy Smart Contract. The contract manages the rest, creating a private on-chain account for the user.

For transaction execution, the user generates a zk-SNARK proof and submits it along with the encrypted transaction details. The Proxy Smart Contract verifies the proof, executes the transaction, and credits the tokens to the user's account, providing a simple, seamless user experience.

Withdrawals are equally straightforward. The user can withdraw their tokens to their original deposit address at any time, with the Proxy Smart Contract managing the process and maintaining privacy.

IX. Conclusion

Shielded Accounts represent a significant advancement in privacy-preserving DeFi. By combining the robustness of smart contracts with the privacy capabilities of zk-SNARKs, Shielded Accounts allows users to interact with the DeFi ecosystem in a secure and private manner, while also maintaining regulatory compliance.

Shielded Accounts open up a new realm of possibilities for the DeFi space, allowing more users to take advantage of the benefits of DeFi without sacrificing their privacy. As the DeFi space continues to grow and evolve, innovations like Shielded Accounts will be key to ensuring that the benefits of DeFi can be enjoyed by all, while also adhering to the necessary regulatory requirements.

X. References

[1] Parno, B., Gentry, C., Howell, J., & Raykova, M. (2013). Pinocchio: Nearly Practical Verifiable Computation. 2013 IEEE
Symposium on Security and Privacy. Retrieved from https://doi.org/10.1109/sp.2013.47

[2] Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized

Anonymous Payments from Bitcoin. 2014 IEEE Symposium on Security and Privacy. Retrieved from https://doi.org/10.1109/sp.2014.36

[3] Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018). Bulletproofs: Short Proofs for Confidential Transactions and More. 2018 IEEE Symposium on Security and Privacy (SP). Retrieved from https://doi.org/10.1109/sp.2018.00020

[4] Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2019). Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive. Retrieved from https://eprint.iacr.org/2018/046.pdf

[5] Groth, J. (2016). On the Size of Pairing-based Non-interactive Arguments. EUROCRYPT 2016: Advances in Cryptology. Retrieved from https://doi.org/10.1007/978-3-662-49890-3_31

[6] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

[7] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[8] Wood, G. (2014). Ethereum: A Secure Decentralized Generalised Transaction Ledger. Ethereum Project Yellow Paper.

[9] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy. Retrieved from https://doi.org/10.1109/sp.2015.14

