ZkFundMe - A Zero-Knowledge Proof and Smart Contract Based Donation Platform

Ivan Dimitrov
Fraunhofer Institute for Applied Information Technology FIT
Schloss Birlinghoven
53754 Sankt Augustin, Germany
ivan.dimitrov@fit.fraunhofer.de

Diana Dabboussi
Fraunhofer Institute for Applied Information Technology FIT
Schloss Birlinghoven
53754 Sankt Augustin, Germany
diana.dabboussi@fit.fraunhofer.de

Mikolaj Radlinski
Fraunhofer Institute for Applied Information Technology FIT
Schloss Birlinghoven
53754 Sankt Augustin, Germany
mikolaj.pawel.radlinski@fit.fraunhofer.de

***Abstract*—ZkFundMe introduces a donation platform that leverages zero-knowledge proof technology in a decentralized framework. This platform enables individuals to create donation campaigns for various crises. By verifying their identity and sharing images and descriptions, campaign creators store data securely on the blockchain. Campaigns are publicly accessible, allowing users to donate discreetly using zero-knowledge proofs, ensuring donor privacy and effective funding for issuers. The application eliminates gas fees via a paymaster system. This innovation reshapes donation dynamics by uniting security, privacy, and community support.**

***Index Terms*—Blockchain accounts, Externally owned accounts, Account Abstractions, Smart contract accounts, Zero-klnowledge proof, Donation, Charity, Blockchain**

I. Introduction

This paper is about the transformative potential of blockchain technology, in particular zero-knowledge proof technology, in the context of charity and crowdfunding platforms. In recent years, the intersection of blockchain technology and crowdfunding has given rise to novel platforms that seek to revolutionize the way individuals access financial aid during crises and urgent situations. An emerging hypothesis is that blockchain technology can help charities increase stakeholder trust in their fundraising activities [3]. While the role of blockchain technology in markets has been widely explored, interest in its charity sector applications has grown [6]. The landscape of charity is about to undergo a transformation, driven by the growth of blockchain technology, which has the potential to redefine the dynamics of donation platforms. In particular, the incorporation of zero-knowledge proof technology is leading to a new era in which authenticity, privacy and operational efficiency are improved. Among these platforms, ZkFundMe emerges as a pioneering solution, offering a decentralized donation ecosystem driven by zero-knowledge proof technology and addresses the challenges of authenticity, privacy, and security in crowdfunding campaigns by implementing a range of features.

II. Motivation

In the evolving landscape of technology and fundraising organisations, the fusion of blockchain technology and charity has proven to be a powerful facilitator of transformative change. In this context, the ZkFundMe project was created at the ETHGlobal Hackathon in Paris 2023. This paper addresses the implementation and execution behind this solution and highlights the impact in the field of charity. One important aspect is the technical implementation of trust. The smart contracts ensure transparency and traceability and build trust by enabling donors to track the use of their contributions. In addition, the use of zero-knowledge proofs (ZKPs) increases donor anonymity, addressing privacy concerns and appealing to a wider range of donors. These technical features significantly increase user acceptance. They build trust among donors who value transparency and accountability, while appealing to privacy-conscious donors. On a societal level, this technology promotes a culture of trust, leading to increased participation and a positive societal impact in the charity sector.

III. Problem Statement

In the field of fundraising and charity initiatives, traditional methods face a number of challenges that undermine their effectiveness and credibility. Prevailing paradigms face obstacles in proving the authenticity of campaigns and validating the identity of recipients, allowing for misleading or misrepresented appeals. In addition, concerns remain about the confidentiality of donor and recipient data, exacerbated by centralised systems that are vulnerable to breaches. The burden of inefficient transaction processes, particularly gas fees, impedes seamless interactions and diverts resources from their intended donation actions. Given these systemic shortcomings, there is an urgent need for innovative measures to address them. The connection of blockchain technology and zero-knowledge proofs presents an opportunity to fundamentally change the landscape of donation platforms. As societal demands for trustworthy, streamlined and inclusive forms of support continue to grow in importance, this paper explores the transformative role of ZkFundMe in depth. By integrating these emerging technologies, this platform is able to improve existing challenges and bring about a paradigm shift in the efficiency and sophistication of donation actions.

IV. Related Work

Within the scope of related studies, the literature consistently emphasizes the transformative capacity of blockchain technology within the traditional donation supply chain. The potential of blockchain is to manifest its ability to accelerate transaction processing, enhance the fluidity of donated resources, establish equitable economic redistribution, and significantly reduce administrative costs. Davies (2015) [4] explores this transformative potential, a notion reinforced by the comprehensive analysis put forth by MercyCorps (2017) [8].

One driving technology is the use of zero-knowledge proofs, which ensure security by validating the authenticity of a transaction without revealing the executing party [5]. Further, zkBOB is a platform that uses this technology to ensure private payment methods for any use case [1].

V. Proposed Solution

The proposed solution is designed to facilitate decentralized fundraising on the Polygon Mainnet blockchain, employing the MetaMask wallet for secure authentication and connection to the blockchain. This donation platform contains two different user roles: Campaign Creators and Donors, each with specific functionalities and permissions.

A. Campaign Creator Role:

- Authentication and Verification: Campaign Creators authenticate via MetaMask and verify their personhood using Worldcoin ID.
- Campaign Setup: They can create campaigns by uploading a picture, adding a title and description.
- Privacy and Security: Optionally, Campaign Creators can employ zkBob addresses for enhanced financial privacy.
- Fund Reception: Campaign Creators receive donations in USDC, a blockchain based stablecoin currency, that simplifies donations.

B. Donor Role:

- Authentication: Donors log in via MetaMask for secure access.
- Campaign Selection: They browse and choose campaigns to support.
- Donation Process: Donors enter their desired donation amount and seamlessly complete the transaction. This comprehensive solution ensures efficient and secure decentralized fundraising, fostering trust, transparency, and privacy for both Campaign Creators and Donors.

VI. Implementation

In this section, we dive into the technologies and mechanisms that drive the ZkFundMe platform.

Technologies and Tools Used

A. Polygon Mainnet

The backend of the ZkFundMe platform is powered entirely by the Polygon mainnet blockchain. The fundamentals of the underlying blockchain provide a foundation for processing donation transactions and campaign-related operations. Utilizing a Layer 2 solution, the platform achieves fast and cost-effective transactions, enhancing the user experience for both donors and campaign creators.

B. Introducing the Paymaster: Simplifying Transactions

A key aspect of our implementation is the paymaster, which is a smart contract designed to pay for transaction fees for campaign creators. This innovation relieves the campaign creator from covering transaction fees, which allows for an easier and cost-free campaign creation process. When a campaign creator wants to store a campaign on the blockchain, the paymaster smart contract steps in to cover the necessary gas fees. As a result, campaign creators can effortlessly set up their campaigns, with the paymaster ensuring the seamless storage of campaign data on the Polygon blockchain.

Through the utilization of the paymaster smart contract, the ZkFundMe platform promotes accessibility and usability. Campaign creators can focus on their initiatives without concerning themselves with transaction fees and complexities. The paymaster's deployment on the Polygon mainnet further aligns with our commitment to efficiency and user experiences.

C. Decentralized Content Storage with IPFS

To securely store campaigns, the ZkFundMe platform utilizes the InterPlanetary File System (IPFS) for storing multimedia content. IPFS breaks files into smaller pieces, each with a unique identifier. This decentralized approach guarantees content availability and imutability, supporting campaign credibility.

D. Zero-Knowledge

Within the field of cryptographic methods on blockchain systems, the ZkFundMe platform makes use of zero-knowledge proofs (ZKPs) to enhance data privacy. Specifically, the platform employs zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) — a modern cryptographic technique that checks the truth of statements without revealing the base information [7]. Zk-SNARKs are non-interactive proofs that are short and computationwise simple to verify. They are designed to be quick and compact without sacrificing security. One of the standout features of zk-SNARKs is that they can verify a statement's truth without showing the actual information behind it. This feature is crucial for keeping transaction details private.

ZkFundMe incorporates the underlying technology of zkBOB for its zero-knowledge capabilities [1]. ZkBob uses zkSNARKS to anonymize senders, receivers, and amounts when transferring stable funds. The transfer verifier circuit proofs the following conditions [1] :

1) Every input note is distinct.
2) Input notes are unique.

3) Output notes are unique or blank (all fields equal zero).
4) "tx" is signed, and the signer is the owner of input account, output account, and input notes.
5) Nullifiers correspond to notes.
6) "out" commitment is the root of merkle subtree of output account and notes.
7) Input account and notes should be inside anonymity set (have valid merkle proofs) or blank (all fields of account excluding η are zeros, balance of note is zero).
8) For non-empty input notes, their position in the merkle tree should fit within a specified range, determined by the input and output account indices.
9) Information about public balance changes, XP changes, and the size of the set they belong to is held in a specific δ input. This data uses a little-endian format and two's complement for signed types. If these values are negative, they're displayed as corresponding field elements.
10) Sum of all balances (with negative signs for outputs) should be zero.
11) Account indices have constraints: the input account index should be less than or equal to the output account index, which in turn should be less than or equal to δ.i.
12) Lastly, there's a set equation for XP that ties together various account indices, positions, and balance changes. When computed, the result should be zero.

An interesting feature in the zkBOB implementation is that each new created account does not utilize static addresses. To receive funds, users must create and offer discrete private addresses. Ideally, a unique private address is generated for each incoming transaction. Multiple private addresses stemming from a single account cannot be interconnected or traced back to the main account. Only the account holder can verify that a private address is linked to their account.

E. "Worldcoin Authentication": A Distinctive Identity Verification

Worldcoin Authentication forms the core identity verification mechanism within the ZkFundMe platform. This approach utilizes the principles of zero-knowledge proofs (ZKPs) and advanced cryptography, which cooperatively interacts with the Worldcoin authentication system [2].
Worldcoin stands as an identity framework, enabling users to authenticate their unique existence while preserving their anonymity. This framework operates through a digital passport known as the *World ID*, which serves as an exclusive and confidential representation of an individual's identity. The proof generated through the protocol is also called *Proof of Personhood* [2].

1) The Authentication Process in ZkFundMe:

- **QR Code-based Initiation:** Within the ZkFundMe environment, the authentication process starts off with the display of a QR code on the screen. This QR code is a gateway to the World App's authentication mechanism.
- **World App Interaction:** To authenticate themselves, users use the World App, which is a key component of the Worldcoin ecosystem. By scanning the QR code using the World App, users initiate the authentication process.
- **Zero-Knowledge Proof Transmission:** Once the QR code is scanned, the World App generates a zero-knowledge proof, initiating the user's authentication. This proof is subsequently forwarded to the ZkFundMe frontend.
- **Frontend to Smart Contract:** The ZkFundMe frontend takes care of transmitting the zero-knowledge proof to the ZkFundMe smart contract. Within this transaction, the zero-knowledge proof is offered for verification.
- **Verification on Smart Contract:** The zero-knowledge proof validation takes place within the ZkFundMe smart contract. This verification step confirms the authenticity of the user's identity.

2) Iris Scanning: The Foundation of Authentication: Central to the success of this authentication approach is the requirement of iris scanning using the *Worldcoin Orb*. Prior to engaging with the "Worldcoin Authentication" mechanism, users must have their iris scanned by the Worldcoin Orb, which is a process that adds an extra layer of security and identity validation. This process is necessary in order to store the hash of the iris data on the underlying blockchain.

Through the interplay of the World App, zero-knowledge proofs, and the Worldcoin Orb, "Worldcoin Authentication" forges a robust bridge between identity verification and privacy-preservation within the ZkFundMe platform.

VII. Evaluation

The evaluation encompasses two principal dimensions: Scalability and Functionality.

1) Scalability:

- **Base Foundation:** The utilization of Polygon mainnet provides the platform with a reliable foundation, positioning it well for growth. This means it's built to handle an increasing number of users and new activities.
- **Efficiency and Cost:** By adopting a Layer 2 solution, transaction speeds are notably fast, and costs are kept low. For users, this translates to smooth interactions without heavy expenses.
- **Paymaster's Role:** A significant advantage is the paymaster feature. Acting as a financial helper, it covers certain costs, allowing users to begin campaigns without the immediate need to deposit digital tokens. This could ease the onboarding process for many users.

2) Functionality:

- **Data Storage:** Implementing IPFS as the platform's storage mechanism offers a decentralized and sturdy solution for preserving information. This approach not only secures user data but also maintains its integrity, enhancing the platform's reliability for its users.
- **Privacy Enhancement:** The platform's use of Zero-Knowledge tools is a step forward in protecting user

details, ensuring privacy without compromising functionality.

- **Identity Verification:** Worldcoin offers a unique method for confirming user identities. While it ensures users are real, it does this without exposing sensitive personal details, effectively balancing user verification with privacy concerns.

The platform exhibits strengths in its choices for scalability and functionality. However, as with any system, ongoing monitoring might be needed to ensure consistent performance as the user base grows and tech landscapes evolve.

VIII. Conclusion

In this study, we've unveiled the "ZkFundMe" platform, blending emerging technologies to reimagine donation initiatives. Leveraging the Polygon mainnet blockchain, IPFS for decentralized content storage and zero-knowledge proofs provided by zk-Snarks, it drives operations. Notably, the introduction of a paymaster smart contract on the Polygon mainnet simplifies campaign initiation.

At the core, Worldcoin Authentication redefines user identity verification through zero-knowledge proofs (ZKPs) and the World ID. Users confirm their identity by scanning QR codes with the World App, coupled with iris scanning via the Worldcoin Orb.

Our findings underscore the promise of emerging tech in securing, enhancing transparency, and expanding accessibility in donation platforms. Worldcoin Authentication sets a precedent for privacy-conscious verification methods. Future work may involve further security measures, scalability, and deeper integration within the Worldcoin system.

In conclusion, ZkFundMe pioneers novel solutions at the intersection of privacy, trust, and accessibility in the digital donation landscape.

IX. Open Questions

Looking ahead, ZkFundMe's vision is to evolve into a complete, real-world donation platform. This transition includes the integration of secure payment gateways to facilitate actual financial transactions combined with strict regulatory compliance - a critical step in realising potential impact. Future work will look at user-centered design principles and develop interfaces that are engaging and intuitive. Research and development efforts are focused on strengthening the platform's defences to ensure the highest possible security of user data and transactions. To further empower users, future work will introduce campaign filtering methods. These tools will enable donors to refine their selection of campaigns based on specific criteria, enhancing the overall donation experience and ensuring that contributions align with donors' values and interests.

Data science tools will aid in understanding user behavior, optimizing platform performance, and providing insightful analytics. Such data-driven insights can enhance decision-making, campaign strategies, and the overall effectiveness of the platform.

Beyond its current scope, ZkFundMe concepts and technologies hold potential across various industries. Future research will explore applications in identity verification, secure access control, and privacy-preserving authentication, expanding the platform's reach and societal impact.

Overall, ZkFundMe is an innovation at the intersection of blockchain, privacy and user trust. These proposed future directions provide the compass that will help to create a robust, secure and adaptable platform for real-world donations, while continuing to push the boundaries of what technology can achieve in the digital age.

X. Acknowledgment

This research was supported by Fraunhofer FIT, Blockchain Reallabor. We are grateful to have had the opportunity to implement this project. Their contributions were instrumental in the successful completion of our research.

References

[1] Transfer verifier circuit overview. https://docs.zkbob.com/implementation/zksnarks-and-circuits/transaction-verifier-circuit, Accessed September 15, 2023.

[2] Worldcoin docs. https://docs.worldcoin.org/, Accessed September 15, 2023.

[3] Andrea Christie. Can distributed ledger technologies promote trust for charities? a literature review. *Frontiers in Blockchain*, 3:31, 2020.

[4] Rhodri Davies. Giving unchained: Philanthropy and the blockchain. 2015. *Charities Aid Foundation*, 2015.

[5] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, 1994.

[6] Sanjit Podder, Partha Roy, Prashanth Tanguturi, and Saurabh Singh. Blockchain for good: 4 guidelines for transforming social innovation organizations. Technical report, Accenture Labs, Bangalore, India, 2017. Accessed August 14, 2023.

[7] Christian Reitwiessner. zksnarks in a nutshell. *Ethereum blog*, 6:1–15, 2016.

[8] Ric Shreves. A revolution in trust: Distributed ledger technology in relief and development. *Mercy Corps*, 2017.