Perpetual Powers of Tau Project

Privacy & Scaling Explorations

November 30, 2023

Contents

1 Abstract

The Perpetual Powers of Tau Project, an initiative led by the Privacy & Scaling Explorations team, represents a significant advancement in cryptographic trusted setups, primarily focused on enhancing zk-SNARKS (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Building upon the original Zcash ceremony, this project introduces a dynamic system that allows continuous addition of randomness, thereby improving security over time. This report delves into the importance of trusted setups in maintaining privacy and scalability in decentralized applications, the evolution of the Powers of Tau ceremony, and the procedural details of the Perpetual Powers of Tau project. It underscores the project's significance in ensuring

robust and scalable privacy protocols in an increasingly decentralized digital landscape.

2 Introduction

The Perpetual Powers of Tau Project is a significant initiative led by the Privacy & Scaling Explorations team which focuses on improving the multi-party trusted setup, Powers of Tau. The ceremony initially developed by Zcash is a procedure that is performed to generate some randomness used for zk-SNARKS and a variety of cryptographic protocols. The Perpetual Powers of Tau improves upon the initial procedure by allowing parties to continuously add randomness and improve the security of the system over time. The goal is to generate over 530 million powers of tau allowing users to generate zk-SNARK circuits with over 260 million constraints.

3 Importance of Trusted Setups:

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) are pivotal for ensuring privacy and scalability in trustless applications. They allow one party, known as the prover, to prove the validity of a statement to another party, the verifier, without revealing any underlying information about the statement itself. This zero-knowledge aspect is crucial for maintaining privacy, as it ensures that no substantive information is conveyed beyond the proof's validity.

In addition to the privacy properties that zk-SNARKs provide, they are also inherintly succinct. Regardless of the complexity of the statement being proved, the proofs are relatively small in size and quicker to verify than it is to re-execute the original computation. This makes zk-SNARKs exceptionally efficient and scalable, a vital characteristic for decentralized applications where speed and resource efficiency are paramount.

In the zk-SNARK procedure, the prover computes values on a polynomial, critical for the protocol's integrity. To prevent fraudulent proofs, randomness introduced via a trusted setup is key. This setup generates a common reference string (CRS), vital for constructing and verifying zk-SNARK proofs. The CRS ensures the authenticity and security of the proofs, underpinning the zk-SNARK system's trustlessness.

4 Historical Context and Evolution

The Powers of Tau ceremony, foundational to zk-SNARKs, originated with Zcash in 2016, aiming to generate the necessary randomness for secure cryptographic protocols. The initial process was intricate, involving a complex multi-stage protocol with six participants. Each participant contributed to the generation of a part of the cryptographic key material in a way that no single participant could compromise the system. The trust in the ceremony stemmed from the belief that at least one of these participants remained honest and did not leak their part of the key. This ceremony set a precedent for future cryptographic protocols, emphasizing the importance of a secure and transparent setup process.

The Perpetual Powers of Tau project was created as a direct response to the initial ceremony's scalability and security challenges, introducing a dynamic system for ongoing randomness addition. This evolution was necessary to address the growing demands of more complex and larger-scale trustless applications. By allowing continuous contributions of randomness, the Perpetual Powers of Tau enhances the robustness and integrity of cryptographic parameters over time. This ongoing contribution model significantly mitigates the risk of compromise associated with a one-time setup, catering to the evolving security needs in the cryptography space. As this technology continues to mature and expand its horizons, the Perpetual Powers of Tau represents a crucial step in ensuring that privacy and security protocols can scale effectively, adapting to the challenges of an increasingly decentralized world.

5 Powers of Tau

The Powers of Tau setup involves generating two sets of elliptic curve points, labeled G_1 and G_2. These points are derived using an unknown scalar value, s. The length of each set, denoted by n_1 and n_2 respectively, determines the number of points it contains. The points in each set are generated by successive multiplications of s, following the pattern:

$$[G_1, G_1 * s, G_1 * s^2 ... G_1 * s^{n_1-1}]$$
$$[G_2, G_2 * s, G_2 * s^2 ... G_2 * s^{n_2-1}]$$

This sequence creates a structured, yet unknown, progression of points. The security of the setup hinges on the secrecy of s; as long as at least one iteration of s remains unknown, it ensures the integrity of the commitments

to polynomials up to a degree of $n-1$. This setup is critical for zk-SNARKs as it allows provers to securely commit to polynomials.

6 Procedure

The Perpetual Powers of Tau ceremony is orchestrated in sequential rounds facilitated by a coordinator. This coordinator plays a crucial role in maintaining the integrity of the process, ensuring each step is securely followed.

The process commences with the coordinator generating an initial challenge, which is then publicly disclosed. Participants, in a predetermined order, perform cryptographic computations on this challenge adding some randomness. Each computation strengthens the overall security of the setup. Participants then submit their response back to the coordinator, who uses it to formulate a new challenge, thus creating a continuous and interdependent chain of challenges and responses.

As this sequence progresses, each response is verified to ensure its validity as a continuation from the previous challenge. This verification involves a series of cryptographic checks, forming an unbroken and secure chain of data.

In a practical application, when a new zk-SNARK project requires a trusted setup, they utilize the latest response in this chain. This response is examined to authenticate the sequence of challenges and responses. To add an additional layer of randomness and security, a random beacon is applied. This random beacon, which could be a hash of a yet-to-be-mined Bitcoin block or another similar random value, enhances the unpredictability and integrity of the process.

This process can also be thought of as a relay race. In this cryptographic relay, each participant acts like a runner, receiving the challenge (the baton) and adding their unique contribution (a burst of speed) in the form of cryptographic computations. This addition of randomness is akin to each runner's distinct sprint, enhancing the baton's integrity with every handover. Just as a relay race's success hinges on each runner completing their part honestly and effectively, the ceremony's integrity relies on each participant's accurate and secure contribution to this continuous chain of challenges and responses.

7 Security Assumptions

In the Perpetual Powers of Tau trusted setup, the security of the setup is grounded in the honest participation of its contributors. The project operates under the critical assumption that at least one participant in the ceremony

must act honestly and without compromise. This principle is pivotal, as the security of the entire setup hinges on this integrity.

Luckily this assumption in the Perpetual Powers of Tau is significantly mitigated due to the involvement of a larger number of participants. This increased participation diversifies the trust base, substantially reducing the probability of all participants being dishonest or compromised. Consequently, this broadened participation enhances the overall security and reliability of the setup, making it more robust against potential threats or collusion among participants.

Another vital security assumption for any zk-SNARK applications that utilize this trusted setup is the thorough verification of the entire chain of challenges and responses. It is essential that every step in this chain, up to the selected response, was verified to ensure the integrity of the process. Additionally, the selection of an appropriate randomness beacon is crucial. This beacon plays a key role in maintaining unpredictability and fairness in the setup, thereby bolstering the security against potential biases or manipulations that could compromise the cryptographic strength of the zk-SNARK applications relying on this setup.

8 Conclusion

The Perpetual Powers of Tau Project is a significant advancement in cryptographic trusted setups, enhancing the security and scalability of trustless technologies. Its ongoing multi-participant approach fosters a robust and private framework essential for privacy and scaling applications. The project's evolution and impact rely on continued participation and contributions from the community.

To contribute and learn more, please visit the Perpetual Powers of Tau project on GitHub.