The Power of Tau or: How I Learned to Stop Worrying and Love the Setup



Sam Parker

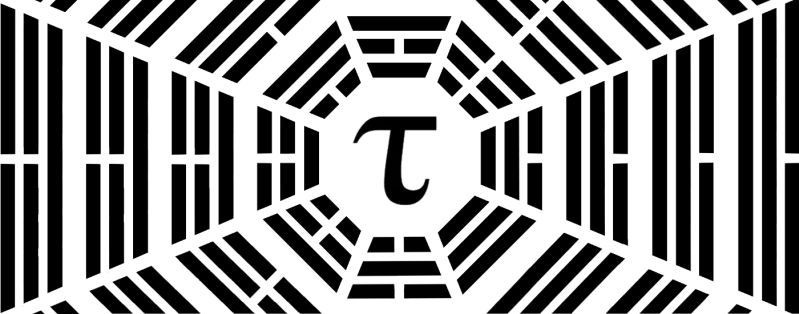
Share on twitter

Share on facebook

Share on telegram

Share on linkedin

Zero-knowledge proofs (ZKPs) have a particularly important history in the context of cryptocurrencies since their inaugural implementations in Zerocoin and Zerocash.



Zero-knowledge proofs (ZKPs) have a particularly important history in the context of cryptocurrencies since their inaugural implementations in [Zerocoin](http://zerocoin.org/media/pdf/ZerocoinOakland.pdf) and [Zerocash](http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf). While early implementations targeted general privacy, ZKPs are only now beginning to be harnessed for many other powerful functionalities besides mere obfuscation. For example, zkRollups enable greater transaction throughput on Ethereum, and recursive proof constructions such as Halo are being used to create a compressed blockchain. Proposals such as [Proof-of-Necessary Work](https://eprint.iacr.org/2020/190.pdf) leverage the capabilities of zkSNARKs to provide security at the consensus layer of the network, and with constructions such as Zexe, ZKP’s enable off-chain computation and even entirely new programming models.

Zero knowledge proofs are often referred to monolithically, but it’s important to remember that there are many different types of ZKPs. Strictly speaking, a ZKP scheme is one that provides the property of “zero-knowledge”, where the verifier of a proof learns nothing about the facts underlying the statement being proved. ZKPs can be interactive, where a verifier interacts directly with a prover, or they can be non-interactive, where the prover can independently generate proofs. There are several classes of non-interactive ZKPs that fulfill that criteria, including:

1. Non-interactive Zero Knowledge Arguments (NIZK)
2. Succinct Non-interactive Zero Knowledge Arguments (SNARG)
3. Succinct Non-interactive Zero Knowledge Arguments of Knowledge (SNARK or sometimes zkSNARK)

zkSNARKs are the most relevant for cryptocurrencies due to their succinctness and efficiency. The first SNARK to be used in production was based on Pinocchio used initially in Zcash. Later, Zcash and several other projects adopted the zkSNARK described by Jens Groth in his [2016 paper](https://eprint.iacr.org/2016/260.pdf) (now colloquially referred to as “Groth16”).

Despite their popularity, zkSNARKs have two major drawbacks.

* First, zkSNARKs which are non-universal (such as Groth16) are specific to a given NP-relation. In other words, proofs are specific to a fixed program, limiting the flexibility of the scheme.
* Second, generating and verifying any zkSNARK proof requires a common reference string (CRS) generated in advance. This process can be thought of as creating a secret that only the system “knows”, any person with knowledge of how the CRS was generated would be able to forge proofs, and therefore break soundness.

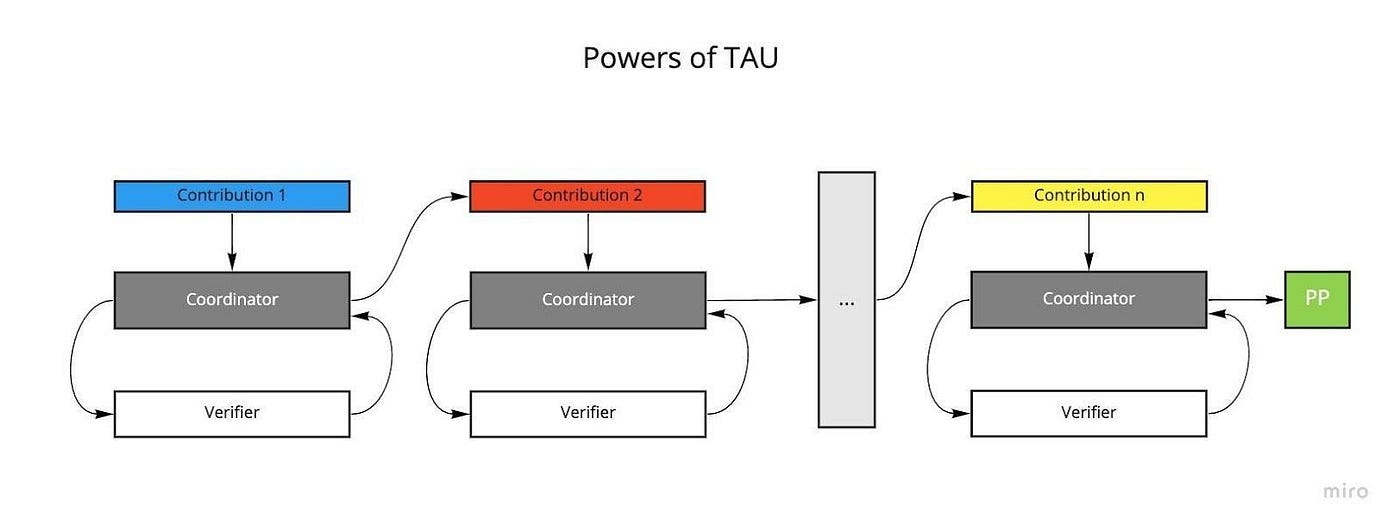
Academic research on universal SNARKs (e.g. [Marlin](https://eprint.iacr.org/2019/1047.pdf), [PLONK](https://eprint.iacr.org/2019/953.pdf), etc) has largely addressed the first problem. But even these still require a CRS. There *are* zero knowledge proof constructions which DO NOT require a CRS, such as STARKs (Scalable Transparent Arguments of Knowledge) and [Bulletproofs](https://eprint.iacr.org/2017/1066.pdf). However, while both STARKs and Bulletproofs have great applications, zkSNARKs (and especially non-universal SNARKs like Groth16) are unbeatable from the standpoint of proof size and verification speed. Of particular interest for cryptocurrencies, verification of zkSNARKs is constant-time. This means that no matter the size of the statement being proven, the amount of work the verifier must do to check the proof remains the same.

Because of this fact, zkSNARKs remain the tool of choice for many privacy-oriented blockchain applications. But the security of those systems largely boils down to how securely the CRS was generated. Therefore, methods of generating the CRS securely in so-called “setup ceremonies” will continue to be relevant. Of course, generating these parameters in a trusted, centralized manner is possible, but incompatible with the goal of decentralization. So far, the preferred technique used in zkSNARK setup ceremonies has been multi-party computation (MPC).

MPC schemes attempt to ensure that no single party generates or is able to gain knowledge of the underlying mathematical structure of the CRS. They accomplish this by requiring the generation process to be shared across as many independent participants as possible in such a way that only a small minority (or even a single individual) need to behave honestly in order for the setup to be secure. In 2015, Eli Ben-Sasson, Alessandro Chiesa, Matthew Green, Eran Tromer, and Madars Virza proposed an improved MPC construction for generating secure parameters even if all but one of the participants has been corrupted. Zcash used this scheme to generate the CRS for the first version of ZCash, “Sprout.” This ceremony was described in this [post](https://electriccoin.co/blog/the-design-of-the-ceremony/) and was also featured in an [episode](https://www.wnycstudios.org/podcasts/radiolab/articles/ceremony) of the U.S. National Public Radio show, Radiolab. Despite its novelty, participation in the ceremony was cumbersome and limited to experts who could be trusted to perform it properly. Moreover, because of the limited participation, it’s generally agreed that the degree of trust required was still too high and contradicted the very ideal of the decentralized system the zkSNARK being set up was meant to secure.

Since then, the goal of setup ceremonies has been to maximize the number of honest, independent participants who can participate in the scheme. Because if there are many independent participants, then, intuitively, the likelihood that all are dishonest is reduced to the point of negligibility. Thus, technical innovations were targeted at scaling up the capability of these ceremonies to support the highest number of participants possible.

One problem with the earlier schemes described above is that the number of participants had to be known in advance. In their MMORPG paper in 2017, Sean Bowe, Ariel Gabizon, and Ian Miers describe a variant on the MPC ceremony for Groth16 setups, which includes two phases. The first we now refer to as “Powers of Tau”, and is a general setup for all circuits up to a given size. The second converts the output of the Powers of Tau phase into a relation-specific CRS. In this scheme a coordinator is used to manage messages between the participants. This scales the process, enabling it to theoretically support hundreds or even thousands of participants. And despite the presence of a coordinator, the output of the MPC can still be independently verified, retaining security. Since the original publication of the paper, Powers of Tau ceremonies have become the industry standard. Projects such as[Filecoin](https://filecoin.io/blog/posts/participate-in-our-trusted-setup-ceremony/), Ethereum ([Semaphore](https://github.com/appliedzkp/semaphore)), and Zcash (“Sapling”) have all used it to generate a CRS for their systems. Figure 1 (below) visually depicts the Powers of Tau ceremony.

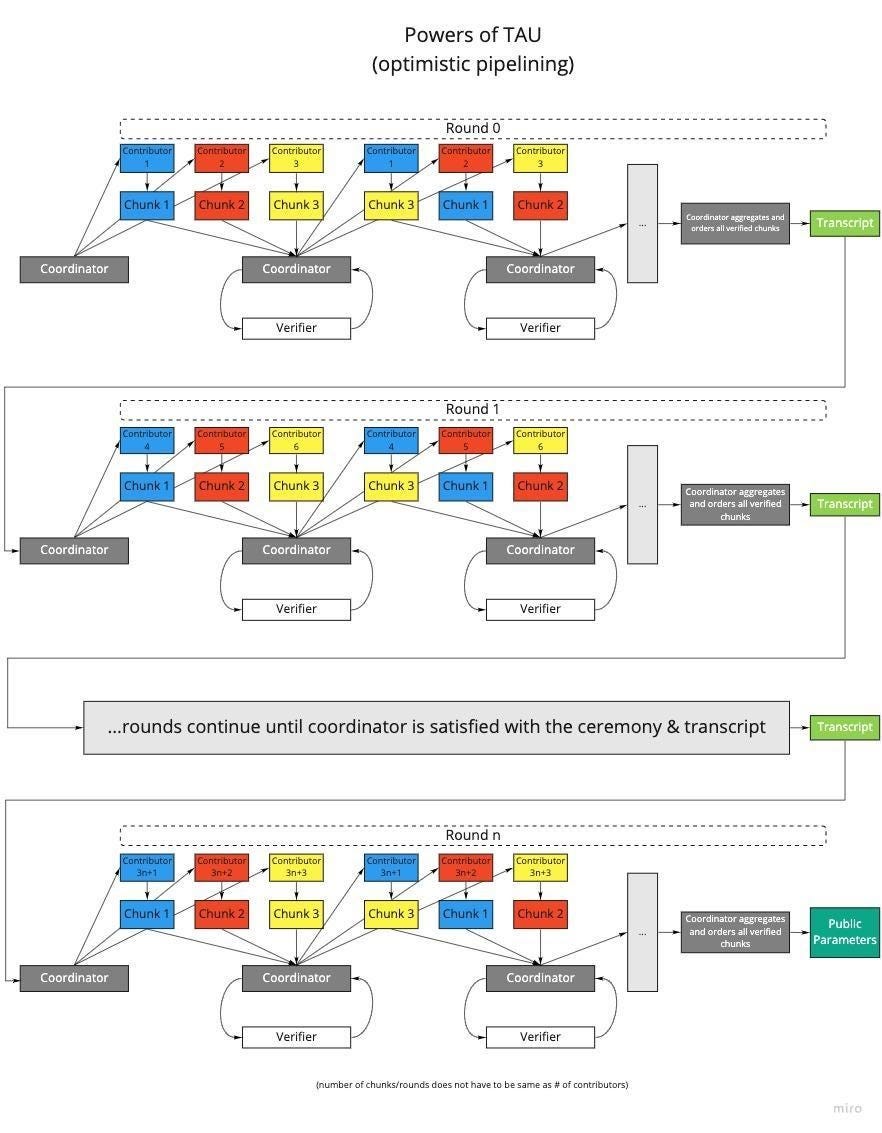


**Figure 1 — Powers of Tau — MMORPG Variant**

Despite its relative popularity, a drawback of MMORPG is that the setup is still a serial process. More specifically, individual participants in the MPC ceremony can only participate one at a time. Because the CRS scales linearly with the size of the circuit, individual contributions can take a long time, and as a result, setup ceremonies are less likely to attract participants. Recently, Justin Drake of the Ethereum foundation has proposed a scheme described as “optimistic pipelining.” The key insight is that contributions can be applied to different parts of the CRS simultaneously, enabling participants to contribute to an MMORPG ceremony in parallel. So rather than having to wait their turn, participants can contribute to a given round at the same time. We describe setups that use this method as “optimistic setups”. Celo’s recent setup ceremony [Plumo](https://celo.org/plumo) used this scheme, and Aleo’s forthcoming setup ceremony uses it as well.

Beyond pure decentralization and security concerns, teams are increasingly viewing these ceremonies as a product in their own right. For example,[Tornado.cash](https://ceremony.tornado.cash/) ran a setup ceremony that enabled users to contribute directly from the web browser, resulting in a record-breaking number of 1114 participants. The success of the Tornado setup shows that, in contrast to prior ceremonies, which were viewed as a necessary evil, modern setup ceremonies that put the user experience front and center not only encourage more contributions, but can be viewed as products in their own right.

The operation of these ceremonies is becoming more streamlined. The original MMORPG scheme used a central “coordinator” to manage messages to and from participants, and assembles the transcript. Historically, this role has been performed manually. But more recently, teams have invested in automating this process (again, see Celo’s [Plumo](https://celo.org/plumo) ceremony and the [Espero](https://www.youtube.com/watch?v=LKbDNc-LrA4) talk by Kobi Gurkan). Not only is this less intensive from a human resources standpoint, it also makes the ceremony more secure since it reduces the chance of error. See Figure 2 (below) for an illustration of how an optimistic setup works.



**Figure 2 — MMORPG in Optimistic Setup Mode**

Though many have argued that the requirement to generate the CRS is a critical flaw for zkSNARKs, there currently is no escaping their efficiency advantages over other ZKP schemes. This is why they remain the industry standard, and why so many teams and researchers have evolved and improved these ceremonies to where we are today. Thanks to improved protocol efficiency, better UX, and automation of tasks such as the coordinator, it’s easier than ever to participate in a setup ceremony, and the number of participants in recent ceremonies reflect that. Whereas the original Zcash ceremony had only six participants, modern ceremonies are able to support many times more. And since only a single honest participant is required for the CRS to be secure, more participants generally equals more security, as each independent member that joins makes complete collusion that much more inconceivable.

It is true that even with a CRS generated through a ceremony, the assertion of security cannot be made mathematical. However, many cryptographic systems are based on assumptions that are somewhat abstract. For example, we’re confident that SHA-256 is a collision-resistant hash function because no one has found a collision **yet**, not because of any mathematical proof (in fact, mathematically we can prove the opposite: that collisions must exist). But SHA256 is so widely used because the odds of a collision are seen to be so astronomically low as to not warrant contemplation.

Similarly, it is challenging (read: impossible) to try to nail down the average probabilities of an individual participant in a setup ceremony behaving honestly in order to mathematically prove the resulting system is secure. However, as the number of participants increases, those odds tend towards vanishingly small even compared to those associated with widely used cryptographic schemes and even with extremely pessimistic assumptions about the participants. In effect, the number of participants is an analog to the security parameter ƛ, used in cryptographic theory as a tunable parameter which provides different “levels” of security for different values ƛ.

Innovations that are making setup ceremonies more efficient are mirrored in the breathtaking pace of ZKP research. Schemes are becoming more efficient, making applications practical, encouraging further innovation and development. This has led to a Moore’s Law-like curve of improvement for ZKPs. Now there are even so-called “transparent” zkSNARKs (such as[Fractal](https://eprint.iacr.org/2019/1076.pdf) and [SuperSonic](https://eprint.iacr.org/2019/1229)) that remove the requirement of a trusted setup. Despite these innovations, the efficiency of existing zkSNARKs such as Groth16 means that they will likely continue to be applied for years to come. Therefore, setup ceremonies can provide an opportunity for a collaborative community celebration of and for the project that is implementing them. So they represent an opportunity to embrace, rather than a necessary evil to overcome.

References

* ZeroCash — <https://ieeexplore.ieee.org/document/6956581>
* Groth16 — <https://eprint.iacr.org/2016/260.pdf>
* Zcash setup ceremony — <https://electriccoin.co/blog/the-design-of-the-ceremony/>
* Zcash setup (Radiolab) — <https://www.wnycstudios.org/podcasts/radiolab/articles/ceremony>
* Original MPC proposal for CRS — <http://www.ieee-security.org/TC/SP2015/papers-archived/6949a287.pdf>
* Second MPC proposal — <https://eprint.iacr.org/2017/602.pdf>
* MMORPG — <https://eprint.iacr.org/2017/1050.pdf>
* Optimistic Pipelining — <https://ethresear.ch/t/accelerating-powers-of-tau-ceremonies-with-optimistic-pipelining/6870>

<https://zeroknowledge.fm/the-power-of-tau-or-how-i-learned-to-stop-worrying-and-love-the-setup/>