Privacy in Blockchain Collaboration using Zero Knowledge Proofs

Dr. Pankaj Dayama

IBM

Zero knowledge proofs (ZKPs) is a technique by which an entity, or prover, with private data provides a verifiable proof to a verifier that certain property/characteristic holds true for that data without revealing any additional information other than the truth of verified property/characteristic. Frameworks for computing succinct zero knowledge proofs without revealing private information are already available. But most practical frameworks suffer from the limitation that, for every new property that the prover and verifier need to establish, they need to go through a costly and time-consuming trusted proof set-up process.

We propose a scalable framework for proving properties/characteristics of private documents in a privacy preserving way. Further, this framework is combined with an innovative protocol that allows all the entities on a blockchain network to participate in the computation of network-level statistics without revealing any private data.