Abstract: Blockchain systems are rapidly gaining traction. Decentralized storage systems like Filecoin are a crucial component of this ecosystem that aim to provide robust file storage through a Proof of Replication (PoRep) or its variants.

However, a PoRep actually offers limited robustness. Indeed if all the file replicas are stored on a single hard disk, a single catastrophic event is enough to lose the file.

We introduce a new primitive, Proof of Geo-Retrievability or in short “GeoPoRet”, that enables proving that a file is located within a strict geographic boundary. Using GeoPoRet, one can trivially construct a PoRep by proving that a file is in several distinct geographic regions. We define what it means for a GeoPoRet scheme to be complete and sound, in the process making important extensions to prior formalism.

We propose GoAT, a practical GeoPoRet scheme to prove file geolocation. Unlike previous geolocation systems that rely on trusted-verifiers, GoAT bootstraps using public timestamping servers on the internet that serve as geolocation anchors, tolerating a local threshold of dishonest anchors. GoAT internally uses a communication-efficient Proof-of-Retrievability (PoRet) scheme in a novel way to achieve constant-size PoRet-component in its proofs.

We validate GoAT’s practicality by conducting an initial measurement study to find usable anchors and also perform a real-world experiment. The results show that a significant fraction of the internet can be used as GoAT anchors. Furthermore, GoAT achieves geolocation radii as little as 1000km.

@misc{cryptoeprint:2021/697, author = {Deepak Maram and Iddo Bentov and Mahimna Kelkar and Ari Juels}, title = {GoAT: File Geolocation via Anchor Timestamping}, howpublished = {Cryptology ePrint Archive, Paper 2021/697}, year = {2021}, note = {\url{https://eprint.iacr.org/2021/697}}, url = {https://eprint.iacr.org/2021/697} }

https://eprint.iacr.org/2021/697