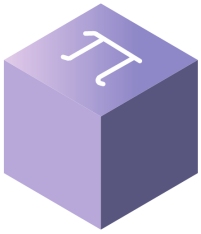

Suyash Bagad

Cryptography & Blockchain Consulting

suyash67.github.io/homepage suyashbagad@protonmail.com

About Us

We are an early stage startup in the R&D stage. Our focus is on helping in bringing the research in the applied cryptography space into production. We provide consultancy services to leading firms in the blockchain space like Aztec Protocol. We have also worked previously with Monero Research Lab and ZenGo Research. We are genuinely passionate about the technology powering the decentralized web and aim to be a contribute our part in it.

Internship Projects for Summer '21

Position: Junior Cryptography Engineer
Duration: 6 to 8 weeks
Starting date: Second or third week of May
Projects:

Name	**Visualising Cryptography**
Type	Engineering
Description	The use of modern applied cryptography in several applications related to peer to peer communication, data storage, digital payments and cryptocurrencies is rapidly growing. For mass adoption of such technologies, there is a need for making it easier for people to understand the technology in the first place. In this project, we wish to build tools which would play a key role in making people understand the core technologies. This project would focus on understanding of the cryptography behind cryptocurrencies such as Monero and MimbleWimble. Further, this project aims to build visualisation tools to explain the cryptography in a lucid manner.
Languages	Python
Requisites[1]	Good understanding of basics of cryptography (Group theory, hash functions, merkle trees, etc)
Eligibility	B.Tech or DD (any branch)
Compensation	₹25,000 per month + performance based bonus

[1] Not a strict requirement but preferable to have.

Name	**Merkle-Tree based Proofs of Reserves**
Type	Research & Development
Description	Proofs of reserves are an important cryptographic tool in enhancing the safety of customer funds in centralized crypto exchanges. Much of the research on proofs of reserves is yet to mature for industry adoption. This project aims to develop a new proof of reserves based on Merkle Trees as an attempt to solve the shortcomings of existing proof of reserves protocols. This project would focus only on cryptocurrencies like Monero and MimbleWimble but could be extended to other blockchains.
Languages	Rust and/or C++
Requisites	Very good understanding of applied cryptography, (zero knowledge proofs, merkle tree based accumulators), Research experience in cryptography and familiarity with Rust is a big plus
Eligibility	B.Tech or DD (any branch)
Compensation	₹30,000 per month + performance based bonus

Name	**MProve+ Implementation in a Monero-fork**
Type	Engineering
Description	MProve+ is a recent proof of reserves protocol for Monero blockchain based on Bulletproofs. We have developed an independent proof of concept of MProve+ in Rust. In this project, we aim to implement the protocol in the Monero source code respository's fork to ensure compatibility with the existing Monero framework. The Monero codebase is in C++.
Languages	C++
Requisites	Familiarity with C++ programming, Prior experience in implementing complex cryptographic systems is a big plus
Eligibility	B.Tech or DD (any branch)
Compensation	₹30,000 per month + performance based bonus

Notes:

- We are a remote-first team, so the internship would be fully remote.
- We do not believe in micro management and so the projects would be fairly independent with necessary guidance.
- Flexible working hours.