Prajwol Gyawali

mail.prajwolgyawali@gmail.com | linkedin.com/in/prajwolrg | github.com/prajwolrg

Experience

Applied Cryptography Engineer Dec 2022 – Present
Venture23 Inc *Sheridan, WY*

- Added bn254 curve operations on goloop to allow for zkSNARK verification on the blockchain.
- Adapted the existing snarkjs library to allow for generation of Java verifier contract.
- Create a proof of concept for anonymous voting on DAO with different voting powers using Pederson commitments.

Blockchain Developer Oct 2020 – Nov 2022
iBriz LLC *Oakland, CA*

- Developed and implemented a comprehensive upgrade plan that ensured seamless migration of existing tokens to the new RMRK standard, while maintaining backward compatibility with existing contracts and applications.
- Led the transition of the platform from a centralized system to a DAO, allowing for greater transparency and community governance by working closely with other developers, stakeholders, and community members.
- Conducted workshop on NFTs, NFT Marketplaces and Royalties for the students of University of Texas, University of Minnesota on as well as the participants of Polkadot Global Hackathon in collaboration with Mousebelt.

Blockchain Intern June 2020 – Sept 2020
Techflow Space *Kathmandu, NP*

- Created contracts for Token SCORE Factory, a web platform for the ICON blockchain where anyone can create IRC-2 IRC-3 standard contracts from their browser without writing a single line of code.
- Published a well-managed course with boilerplate code for on-boarding new developers to the ICON ecosystem.

Projects

Money Market | *Solidity, Ethers, React* July 2022 – Aug 2022

- Implemented the smart contracts of a decentralized lending and borrowing platform, inspired by Aave.
- Authored a three-part article series detailing the mathematics and the economic principles of the platform.

zkHangman | *Solidity, Circom, SnarkJS, NextJS* June 2020 – July 2022

- Utilized the zkSNARK protocol to ensure privacy and confidentiality of the word being guessed, while still allowing the smart contract to verify the correctness of the guess.
- Identified key areas for improvement in existing zkHangman game, including the need for enhanced confidentiality and support for variable word lengths, and developed a solution that addressed both issues.

Roulette | *Solidity, React, Chainlink VRF, Openzeppelin Defender* Sep 2022 – Feb 2023

- Designed and developed a Roulette game in Solidity with robust and granular set of roles and permissions.
- Leveraged Chainlink VRF to ensure provably fair and tamper-proof randomness in the game.
- Implemented gasless meta transactions following ERC-2771 standard utilizing Openzeppelin's Relay and Autotask.

Education

Pulchowk Engineering Campus Nov 2018 – Apr 2022
Bachelor in Computer Engineering *Kathmandu, NP*

Encode Sep. 2022 – Nov 2022
Zero Knowledge Bootcamp *Online*

Harmony zkDAO May 2022 – July 2022
Applied Zero Knowledge Product Building *Online*

Technical Skills

Languages: Solidity, Rust, Circom, ZoKrates, JavaScript, Python, C/C++, Java, SQL (MySQL)
Frameworks: Hardhat, Foundry, React, Node.js, JUnit, WordPress, Material-UI, FastAPI
Developer Tools: Git, Docker, Vim, Remix, VS Code, Metamask
Libraries: Openzeppelin, Chainlink, Circomlib, SnarkJS