Sourabh Aggarwal

sourabhxyz SourabhLight sourabh.xyz
swasti@sourabh.xyz

Education

Indian Institute of Technology, Palakkad[1] 2016 – 2020
B. Tech, Computer Science & Engineering

- Gold medalist, ranked 1^{st} by securing highest CGPA.

Past work & Skills

Haskell

- Article on Segment trees in Haskell, showcasing both lazy & persistent form.

Plutus & Web Development

- Founded adaplays.xyz, a site to play staked games where moves are verified by blockchain.
  1. Key for AES-GCM symmetric encryption algorithm is generated via PBKDF2 algorithm using user's set password. All the random numbers generated (under commit-reveal pattern) are effectively encrypted using this key and stored as an inline datum of UTxO.
  2. Having minimum stake amount to be 3 Ada, cost for minimum UTxO is effectively hidden and not relevant. Increase in transaction cost (44 lovelace per byte) is minimal.
  3. Whole project is as such server-less, could be exported as a static site and run by end user locally with a sole limitation of giving a node provider such as blockfrost. Design can handle up to 10^6 UTxO's per game address.
  4. Parameterized script (parameterized by UTxO) is used to get unique currency symbol (NFT) per game. Minted with first move of game & burned with last. Off-chain code is written to verify whether a found game indeed has an NFT by generating currency symbol with parameters found from datum (of course, check is performed to see whether the token in question is present in UTxO or not). Since finding pre-image of such a hash function is next to impossible (their is also less entropy here as script code & token names are fixed), this is secure.
  5. Project is build with help of:
     * **Next.js** (**React** framework) with **typescript** (~~: any~~).
     * **NextAuth.js**: to manage user session securely and having it synced across multiple windows / tabs.
     * **Chakra UI**: for styling.
     * **Lucid**: To create off-chain code for transactions.
- My portfolio site, sourabh.xyz illustrates the use of framer-motion.

Solidity

- Created 20 hour long course on Solidity, going over official documentation, introducing Ethereum Virtual Machine (EVM) & ethers.js. Covering Hardhat & first 10 challenges of damnvulnerabledefi.xyz.

Zero Knowledge Proofs

- Created a tutorial on zkSNARKs in collaboration with cryptonaukri.com. First part and Second part.

C++ & Competitive-Programming

- Our team, "team_light" secured all India rank 20 in preliminary ICPC 2018.
- Secured all India rank 86 among 4k participants in a programming contest conducted by Johnson & Johnson. Certificate.

Other Honors

China Youth Delegation
Indian Government *2018*

- Selected by the Ministry of Youth Affairs & Sports, Govt. of India among 200 students to represent India as a youth delegate in the "Indian Youth Delegation to China - 2018". Certificate & report.

B. Tech Project Appreciation
IIT Palakkad *2020*

- Received certificate of Merit (given to best three projects per major) in appreciation of work done towards the final year B. Tech project titled, "Tiger to RISC V Compiler" which is a compiler written in Standard ML[2] to compile from extended specification of "Tiger" language to RISC V.

[1] *Indian Institutes of Technology* form India's premier Technology institutions. Admission was secured into this school by being in top 0.4% of roughly 1.3 million applicants.

[2] *From wiki:* Standard ML (SML) is a general-purpose, modular, functional programming language with compile-time type checking and type inference. It is popular among compiler writers and programming language researchers, as well as in the development of theorem provers.