CRIME PATROL

DESIGN DECISIONS

SUBMITTED BY

NITHIN JOHN

RITWHIK C D

AMAL IHSAN

DOCUMENT SCOPE

This document gives the information about how we came up with the idea of developing this application.

PROJECT OVERVIEW

We are making a blockchain based file storage Dapp with controlled access to functionalities on top of the Ethereum blockchain. This means that the immutability factor of the blockchain is used extensively.The Crime patrol is an idea which developed from the thought of preventing the manipulation and the loss of important documents utilising the immutability of blockchain. This led to the question , which document is to be preserved and who should be able to view it. Upon further thought we decided to select the verification process of government approved agencies , if a criminal record exists for a person , as the concept . The optimal approach to implement this seemed to be making a permissioned network with controlled access by issuing tokens.

The access control to the network is controlled by one time issuing a custom token to all the authorized users when they visit the application for the first time.This led to the formation of a function to check that the user already exists in the system. The authorization of the users should be manually done by the admin. The users can only search for the record of a person in the records using some unique id of that person. The records should be added by the police along this the copy of the FIR as entering the crime details can lead to mistakes. The files uploaded will be saved in ipfs and the ipfs hash of it will be stored in the blockchain as part of the associated person’s unique id. At this point we came to the realization that there may be multiple accurances of crime for a person and there by multiple documents needed to be stored under the same unique number which demended an append function to that unique id.

We indented to store the hashes of all the ipfs files into an array of string and return it along with other details of the person to the front end. That idea met with a sudden obstacle as the current version of solidity doesnt support the passing of array of strings, array of structures. We were forced to improvise many things and had to resort to passing all the ipfs hashes as a single string and splitting them at front end.

DESIGN STRATEGIES

- We have provided a structure which contains the details of the criminal including fingerprint hash and criminal record hash. This structure is mapped

using any valid unique identifier (in this case aadhar number). On entering the details, it gets stored in the blockchain.

- The stored data can be retreived for viewing using the unique identifier which we used to store the data.
- The admin can append the data of a specific criminal using the same unique identifier.
- We have also given a provision such that admin can transfer a certain amount of tokens to a user so that the user can get write privileges.
- The controlled access to the Dapp was important for the application and implementing such a thing by regular hardcoding didn't seem optimal. Thus we decided to issue token to the addresses that seem alright for the admin after manual verification and left a field for him to allot such an address with access to token.

- The need to include more than one document to a single person's details led us to the conclusion that we needed to pass an array of string which contains all the addresses of the files associated with the person. Here we hit a little obstacle as the current solidity version doesnt support passing an array of strings or anything with 2D dynamic structure or more for that matter. We had to come up with a solution and had to combine all the addresses into a single string with a seperator and split then and show them seperately at the front end.