## 黑客松比赛版Alibisv

1. 概要

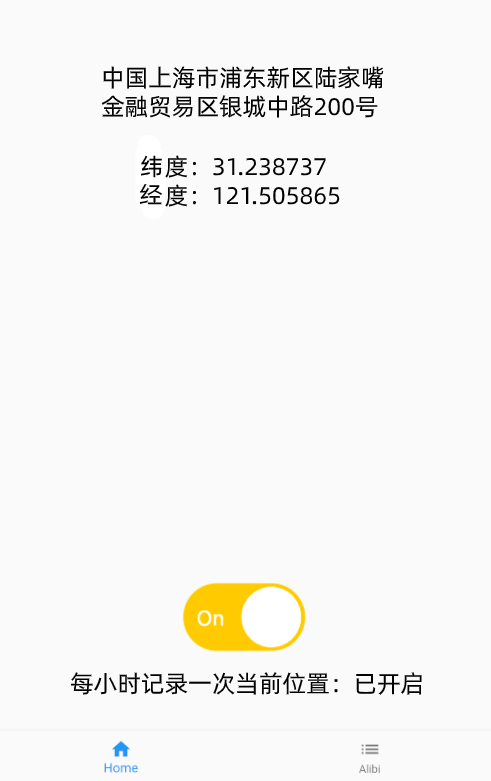
未来是无法预测的，每个人都有可能被卷入一些案件之中成为被怀疑的对象，比如汽车套牌案件，甚至谋杀案，因此有必要为自己的未来上一道保险，我们可以持续记录自己手机的gps信息，这些记录就是我们的不在场证明，当意外发生时这些不在场证明可以解决很多麻烦。但是手机里的记录可以随意更改和伪造，服务器也一样，所以我们需要不可篡改的区块链，将手机的记录的哈希值上传到区块链上，哈希值可以证明记录的真实性。

1. Alibisv设计

Alibisv 是安卓与IOS平台上的App，主要功能是在后台每小时运行一次，每次运行时将GPS信息的哈希值上链，将GPS信息与上链后拿到的Txid保存在手机中。

考虑到评委是外国人，需要做英文版的界面或者国际化。

参加比赛的版本不需要用户付费，因此只有两个页面，首页展示当前位置信息和设置是否开启后台自动记录，AlibiList页显示所有的记录。



首页设计



AlibiList页



Alibi详情页

如果用户经常在不同时区不同语言的国家之间穿行，我们的时间和地址记录就不好处理，所以时间和地址我们不能存当地时间和当地地址，我们只存全球通用的经纬度和UTC时间戳，然后在渲染AlibiList时再将经纬度和UTC时间戳转换为当地地址和当地时间。

1. 哈希算法

计算哈希时需要用到的有

|  |  |
| --- | --- |
| 纬度 | utf8string |
| 经度 | utf8string |
| UTC时间戳 | utf8string |
| 盐 | utf8string |

因为链上的哈希值是公开的，为了防止有人用彩虹表破解这些公开的哈希值导致用户行踪泄露，每次计算哈希都要随机生成一个盐加上去，盐的具体位数看随机算法，dart自带的随机算法只能生成32位随机数。

采用标准的加盐哈希算法计算哈希：

Hmac（SHA256（纬度+经度+UTC时间戳），盐）

哈希256位，记录为HEX格式。

虽然汉语中是“经纬度”，但是实际使用中前面的数字才是纬度，后面的数字是经度。

1. 上链接口

采用打点钱包的接口，post过去就行：<https://developers.dotwallet.com/docs/push/simple>

这个接口只能在比赛版本中使用，因为这个接口需要商户的appid和secret，这两个信息按理是不能放在客户端的。

1. flutter库

安卓上可以让程序周期性在后台运行的库：<https://pub.dev/packages/android_alarm_manager>

配合上一个库需要安装的库，不装程序会崩溃：<https://pub.dev/packages/flutter_plugin_android_lifecycle>

计算哈希用到的HmacSHA256算法库：<https://pub.dev/packages/crypto>

获取gps信息的库：<https://pub.dev/packages/gps>