一块链习 × Blockstack

Class 4

Gavin

gavin@blockstack.com

本课内容

- **项目分析**
  - App-Mining
  - Lander 项目分析
- **Blockstack 存储系统架构总结**
  - 数据定向分享原理
- **Blockstack 整体架构**

项目分析

• 项目分析

- **如何寻找Blockstack 项目**
  - App.co
  - https://theblockstats.com/
- 分析 Blockstack 项目
  - 查看网络流

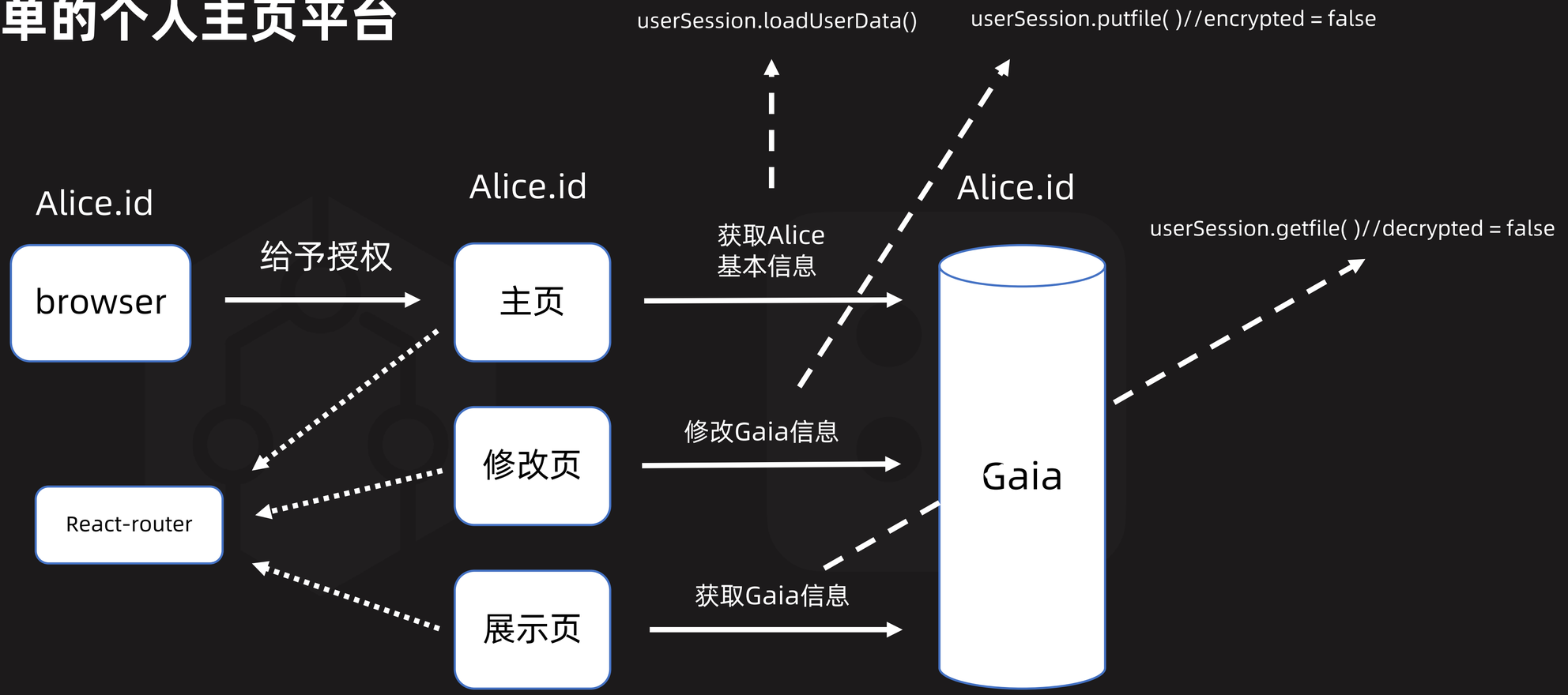
    查看数据存储的位置（用户自己的 gaia 地址？应用自己的 gaia 地址？）
  - 查看数据流

    查看数据存储的方式（加密？明文？部分加密？）

项目分析 - Lander

• Lander

• 简单的个人主页平台



Blockstack 存储架构分析

• Gaia 分析

• Gaia 特性

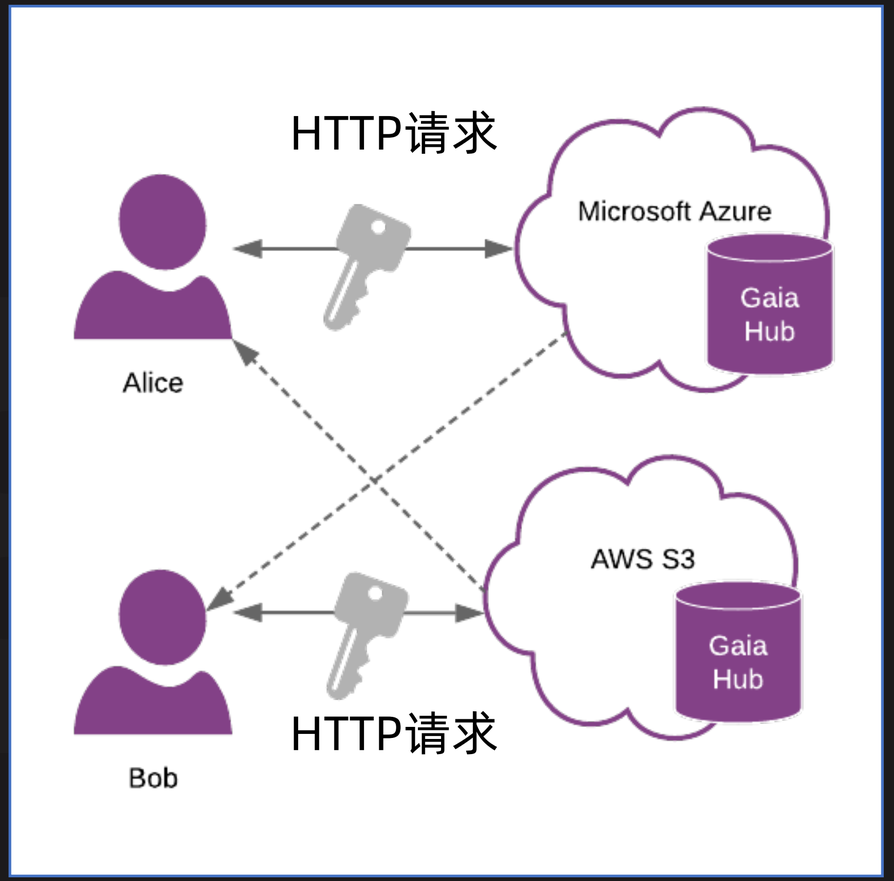
- 提供了基于HTTP的服务协议
- 可以寄托在任何云服务平台上
- 通过DID对应的私钥来授权用户数据

• HTTP API

- 读：GET ${read-url-prefix}/${address}/${path}
- 写：POST ${hubUrl}/store/${address}/${path}
- 参考链接：https://github.com/blockstack/gaia

• CRUD API

- 增：putfile　删：deletefile
- 改：putfile　查：getfile



• Gaia 与开发的相关操作

- **CRUD API**
  - 增：putfile　删：deletefile
  - 改：putfile　查：getfile

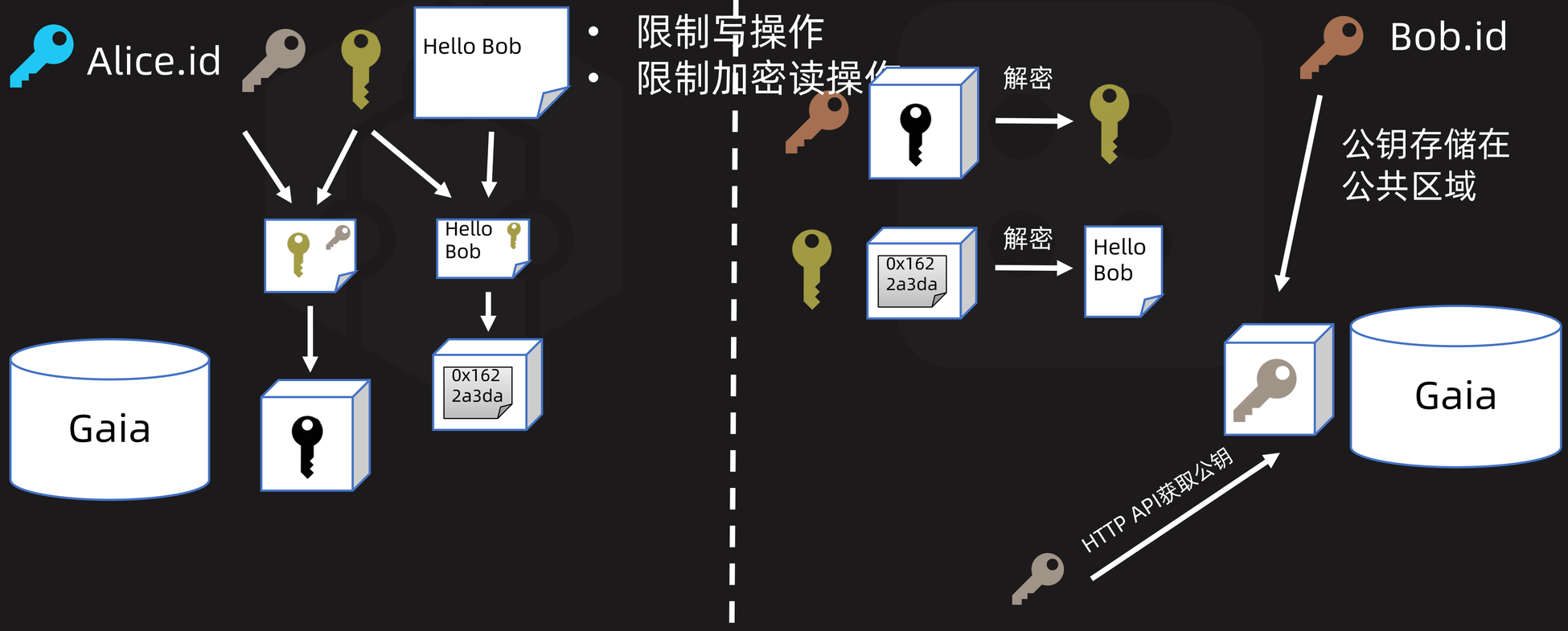
没有传统数据库灵活

- **常见问题与解决方案**
  - 单文件存储应用数据应用逻辑过于繁杂： 在应用内规划数据存储树
    1. 在设计应用初期规划好需要存储到用户端的文件树，在产品服务的不同层级设计不同的文件存储方式（文件名、是否加密等）
    2. 建立一个应用存储公共域名，其对应空间为开放式明文存储，用于管理用户文件信息（随机文件名）

• Feature - 定向数据分享

• 问题描述

1. Alice.id 想向 Bob.id 分享自己 Gaia 数据库中的数据
2. Alice.id 不想分享自己的私钥给 Bob.id
3. 除Bob.id 外，其他人无法解密 Alice.id 要分享的数据



• Feature - 定向数据分享流程

• 问题描述

1. Alice.id 想向 Bob.id 分享自己 Gaia 数据库中的数据
2. Alice.id 不想分享自己的私钥给 Bob.id
3. 除Bob.id 外，其他人无法解密 Alice.id 要分享的数据

1. Bob.id 将公钥 key_Bob 放到公共区域（预处理）
2. Alice.id 生成对称密钥 key_sy，并将对称密钥对文件进行加密
3. 加密后的文件 file_signed 放到公共区域
4. Alice.id 获取 Bob.id 公共区域的公钥 key_bob
5. Alice.id 使用 key_bob 加密 key_sy
6. 加密后的文件 key_sy_bob 放到公共区域
7. Bob.id 获取 Alice.id 公共区域的 key_sy_bob 与 file_signed
8. Bob.id 通过私钥解密 key_sy_bob 为 key_sy
9. Bob.id 通过 key_sy 解密 file_signed 为 file **(END)**

• Feature - 定向数据分享总结

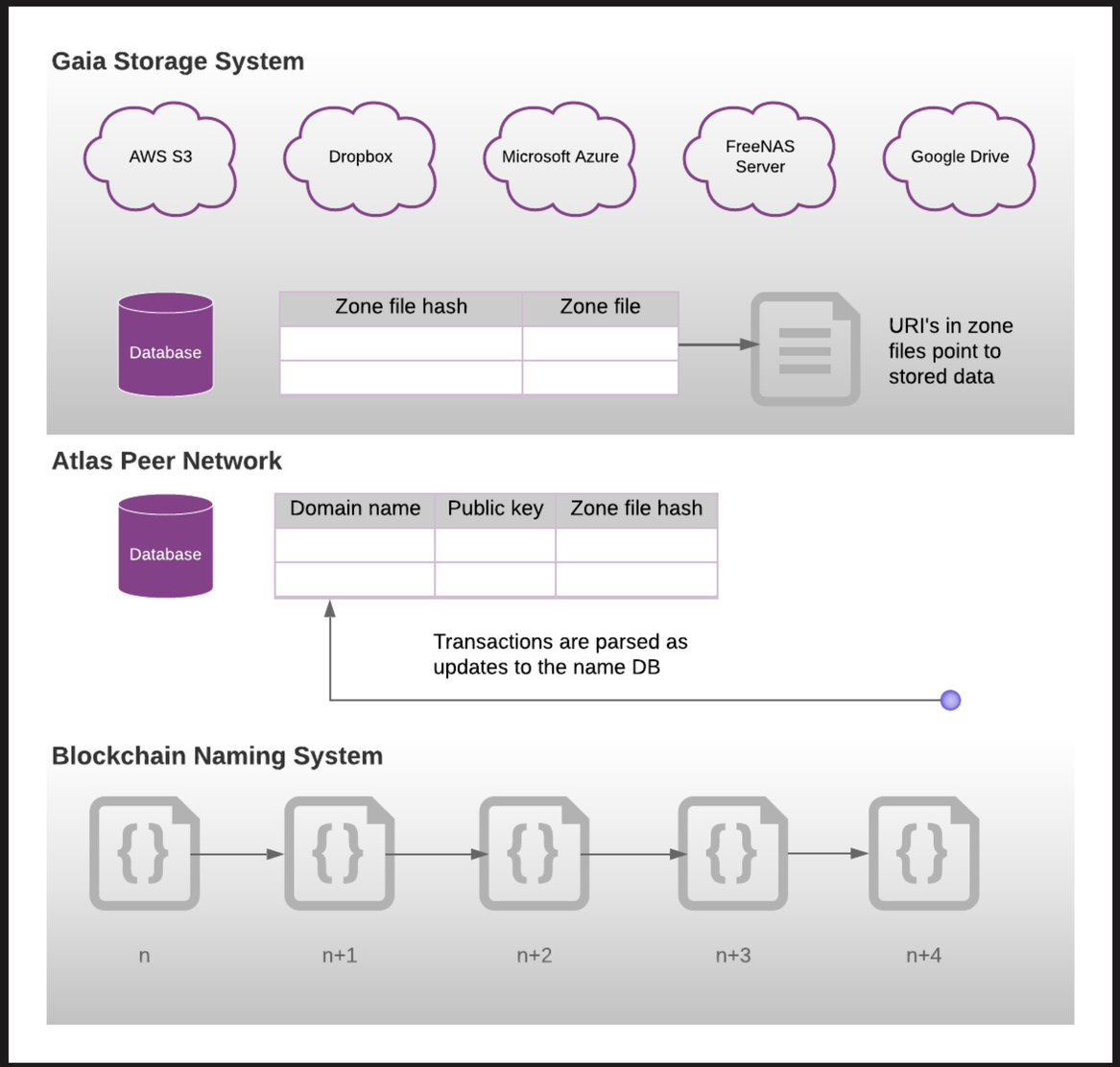
- 用户存储在Gaia的数据是全局可访问的，区别在与读到的信息是否可读（可解密）
- Gaia只提供基于HTTP API的存储服务，复杂的加密解密操作需要应用方自行完成
- Blockstack 提供其他工具（Radiks，collections）来完成开发者需要的特性

- **参考链接**
  - RSA数学推导
    https://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html
  - http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

Blockstack 整体架构分析

• Blockstack 整体架构分析

- 区块链层
  - 域名系统
  - 智能合约
- 路由层 (Atlas)
  - 域名对应 zonefile hash
  - core.blockstack.org 为路由层节点
- 存储层
  - zonefile hash 对应 zonefile
  - zonefile 对应 Gaiahub 存储链接
  - Gaiahub 可以绑定支持HTTP请求的云服务商



课后作业

• 课后作业

- 理解数据定向分享原理
- 给大家三个方向的产品，大家选自己感兴趣的一个做一下项目分析，将产品分析的流程图按照 Github HomeWork 中指定格式发送到仓库中
- 回答思考题目，题目放在 Github HomeWork 仓库 lesson3 文件夹中

  - https://landho.app/ 去中心化搜索引擎
  - https://app.sigle.io/ 去中心化博客
  - https://xordrive.io/ 去中心化网盘