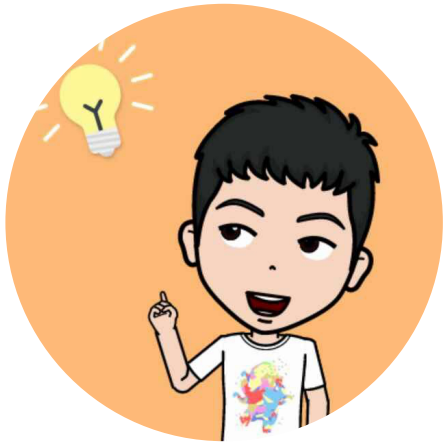
Security Best Practices on Rails



黄金剑 nfreeness

- OTCBTC 风控部主任
- 全栈程序员
- 全栈营线下班第一期

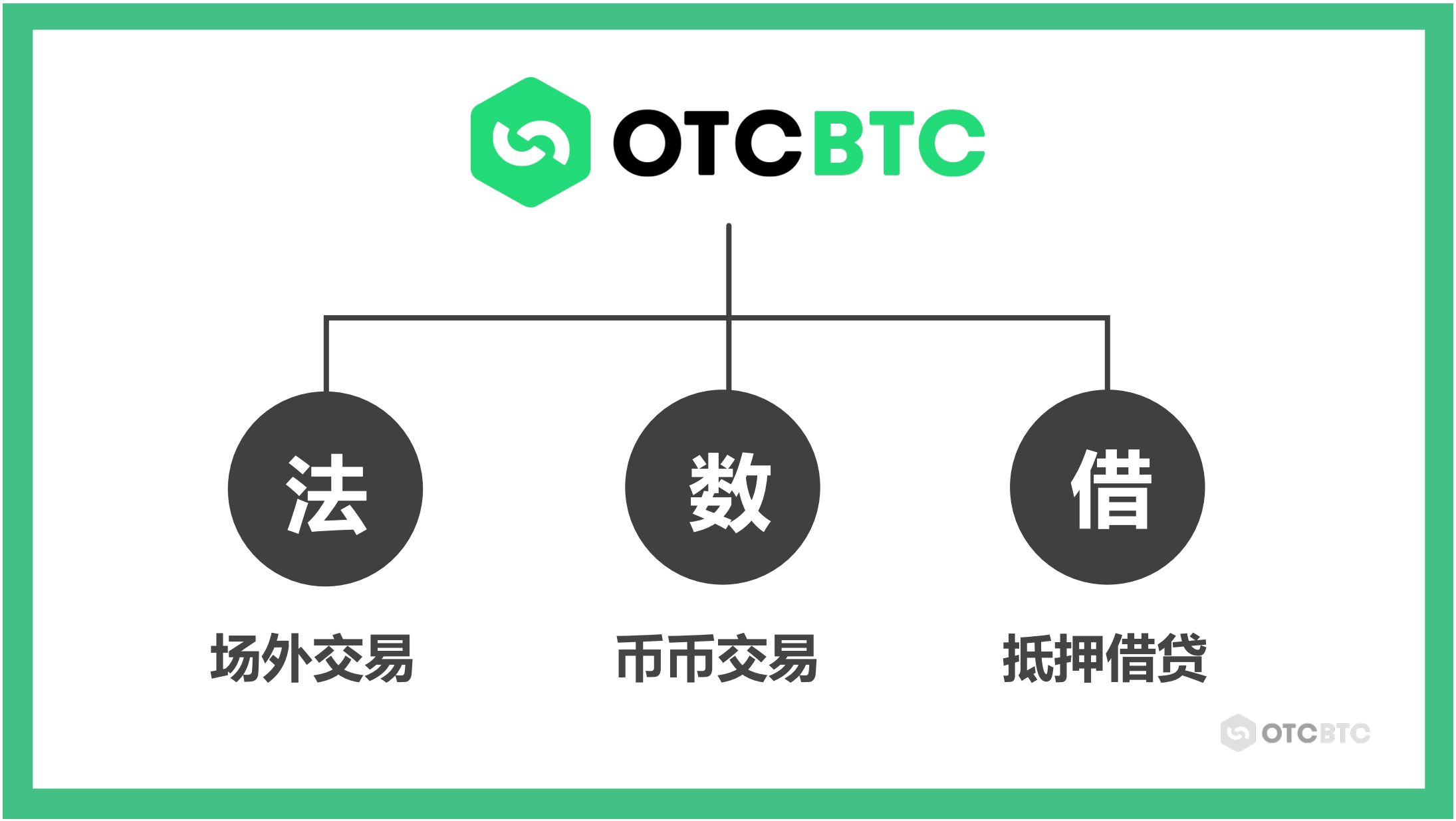
大三学生手头有6000 元，有什么好的理财投资建议？

买比特币，保存好钱包文件，然后忘掉你有过6000元这回事。五年后再看看。


震惊三连
不会吧
真的吗
太厉害了
6000元
3880万
1260万
Sep '13
Mar '14
Sep '14
Sep '17
Mar '18
Sep '18
OTCBTC

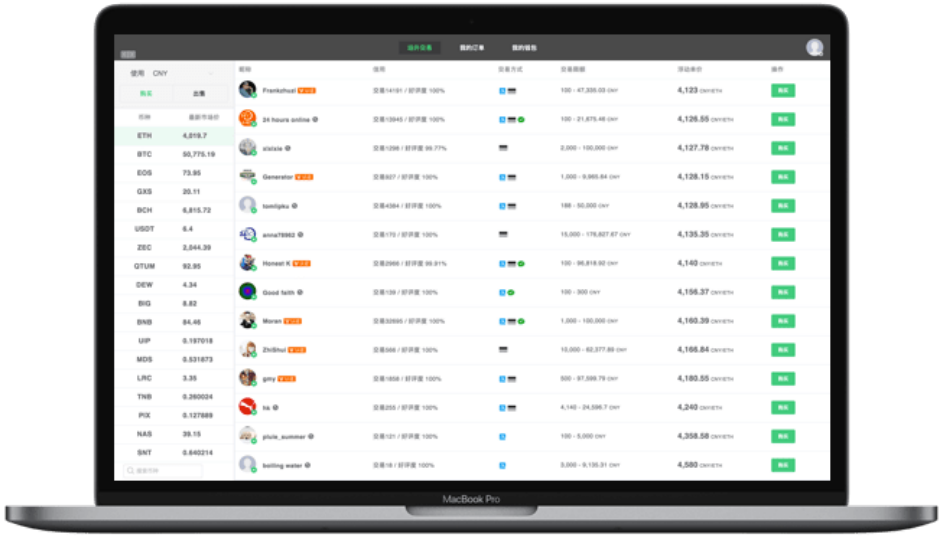
OTCBTC

区块链资产交易平台

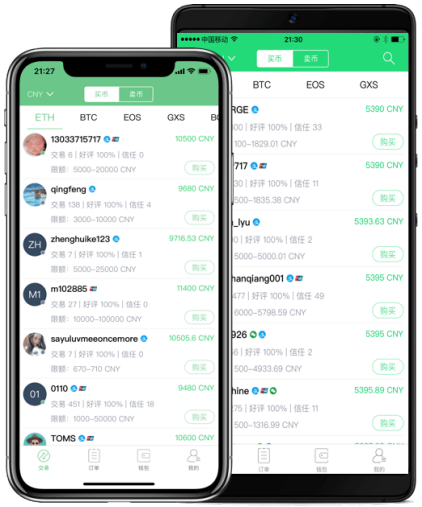

OTCBTC
法
数
借
场外交易
币币交易
抵押借贷
OTCBTC

otcbtc.com otcbtc.io

OTCBTC

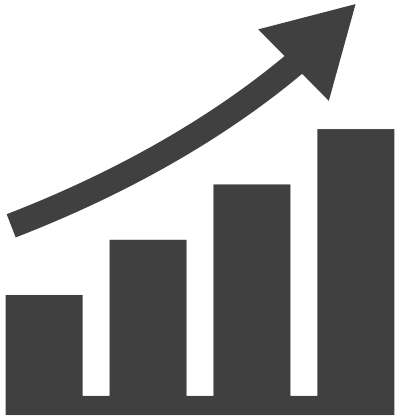


桌面客户端



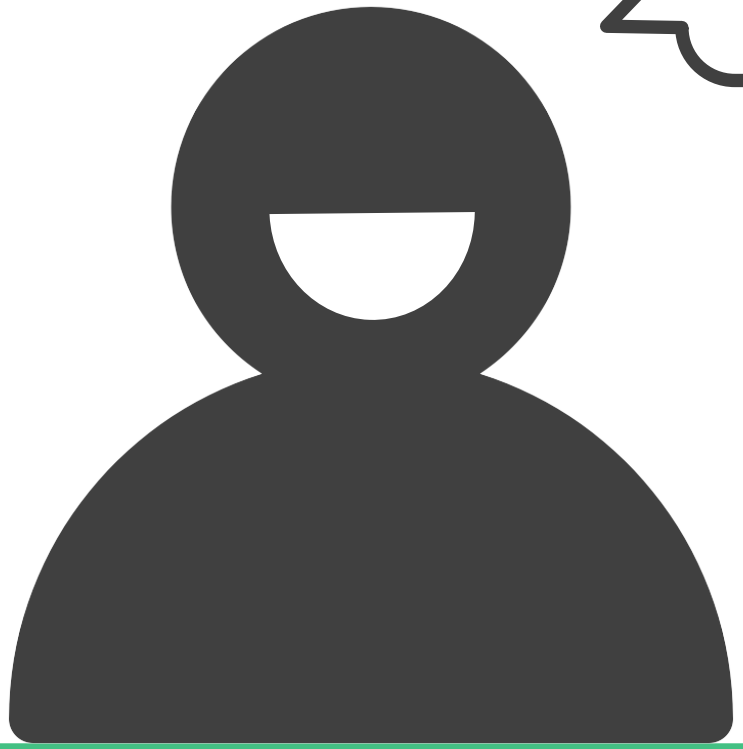
手机APP

OTCBTC



一年营业额 100 亿

主要围绕四个主题



1. 代码安全

2. 资金管理

3. 业务逻辑

4. 第三方服务

Part1. 代码安全

常见攻防手法

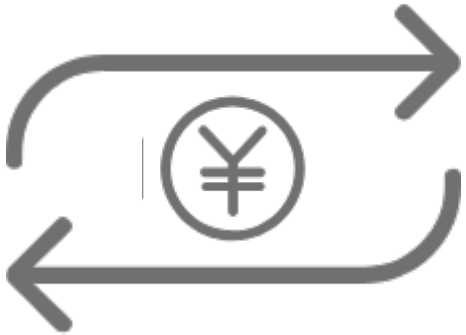
XSS

SQL

Shell

生产环境预警

CI 测试



资金流测试

风控策略测试

智能合约安全

- 智能合约本身的漏洞
- BAI 事件主动赔偿 100+ ETH
- 智能合约风控策略

Part2. 资金管理

数字资产保管

冷钱包 温钱包 热钱包

用户资金安全

用户端主动防御：

1. 高危事件通知

2. 异常设备登录验证

3. 两步验证/短信验证

4. 提币确认邮件

服务端自动防御：

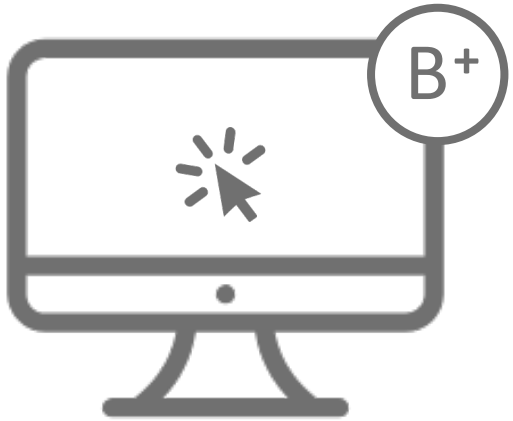
1. 禁止提币缓冲期

2. 自动拦截危险提币

Part3. 业务逻辑

预警机制/系统

- 管理权限细分
- 安全日志
- 高危事件 Slack 通知



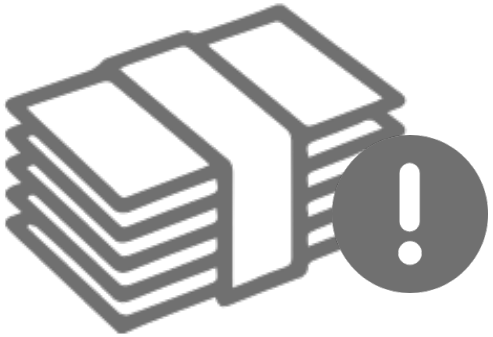
用户行为评级

防止损失—羊毛党

- 影响正常用户的参与
- 无法贡献价值
- 预警系统+活动规则

反诈骗

- 用户行为评级分数
- 诈骗风控策略
- 防诈骗意识/举报系统



反洗钱

- 数字币的匿名特性
- 洗钱风控策略
- 可疑用户身份验证

Part4. 第三方服务

安全审计

白盒

灰盒

黑盒

慢雾科技：智能合约安全、0day 通报等

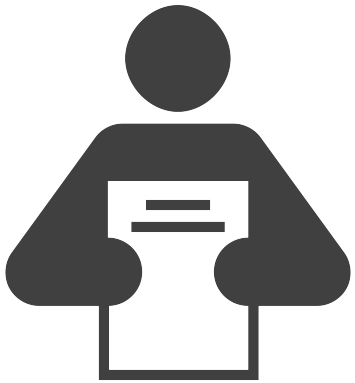
赏金计划：借助群众的力量

Sqreen：WAF 定制化防御

极验科技：行为验证

总结

FAQ



- Xdite :《运营交易所的安全挑战》系列文章
- Sqreen : OTCBTC Case Study

加入高速迭代的世界

hr@otcbtc.com

- 资深后端工程师（API）
- 资深后端工程师（Application）

谢谢聆听