DeFi协议之借贷

Compound&Aave

Keegan / 2022.03.24

课程大纲

- **Compound 借贷协议**
  - 业务模型
  - 利率模型
  - 利率机制
  - 代码解析
- **Aave 闪电贷**
  - 闪电贷原理
  - 执行流程
  - 应用示例
  - 闪电贷攻击

Compound

https://compound.finance/

业务模型

超额抵押贷款

- 由抵押率控制，不同资产有不同的抵押率，最高 82%，最低 0%
  - ETH 抵押率 82%， USDC 抵押率 80%， USDT 抵押率 0%
- 需用户主动选择哪些资产作为抵押品
- 用户的可借额度由其所有抵押品汇总
- 抵押品价值读取自价格预言机
- 贷款资产价值超过抵押资产的抵押率时（即可借额度），则可被清算

cToken

存款凭证

- 用户存款后会得到 cToken，作为存款凭证，也称为生息代币
- 每种标的资产 Token 对应一种 cToken ,如： ETH-cETH 、 DAI-cDAI
- Token - cToken 的兑换率：
  - exchangeRate = (totalCash + totalBorrows - totalReserves) / totalSupply
- 一般情况下，兑换率会随着时间不断增长
- 还款时 ,归还 cToken ,返回 Token ,包括本金+利息， cToken 被销毁

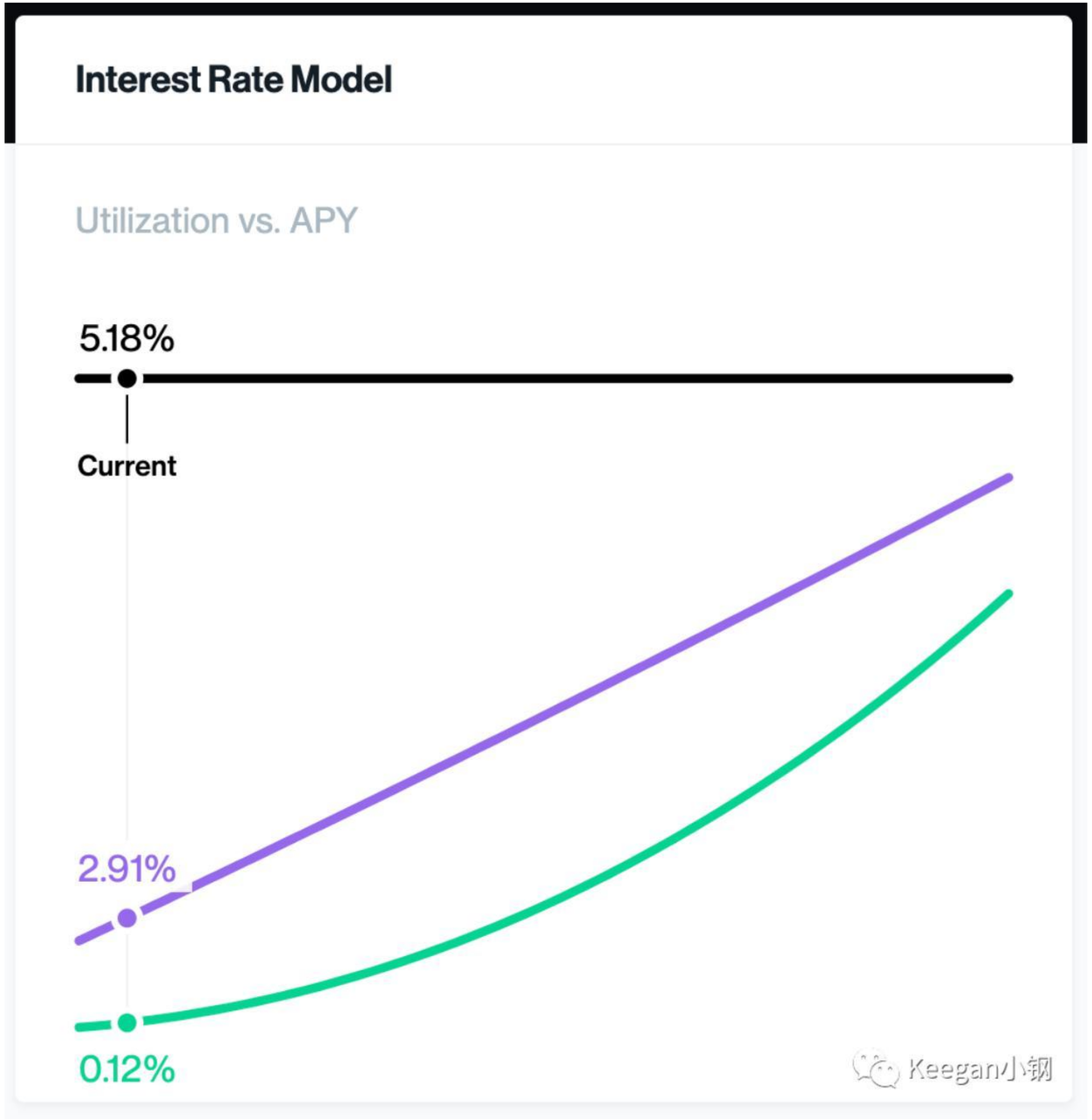
利率模型

供求关系

- 根据单个资产的供求关系，实现有效的利率均衡
- 用资产利用率来衡量供求关系：
  - utilizationRate = borrows / (cash + borrows - reserves)
- 目前主要有两种利率模型
  - 直线型
  - 拐点型

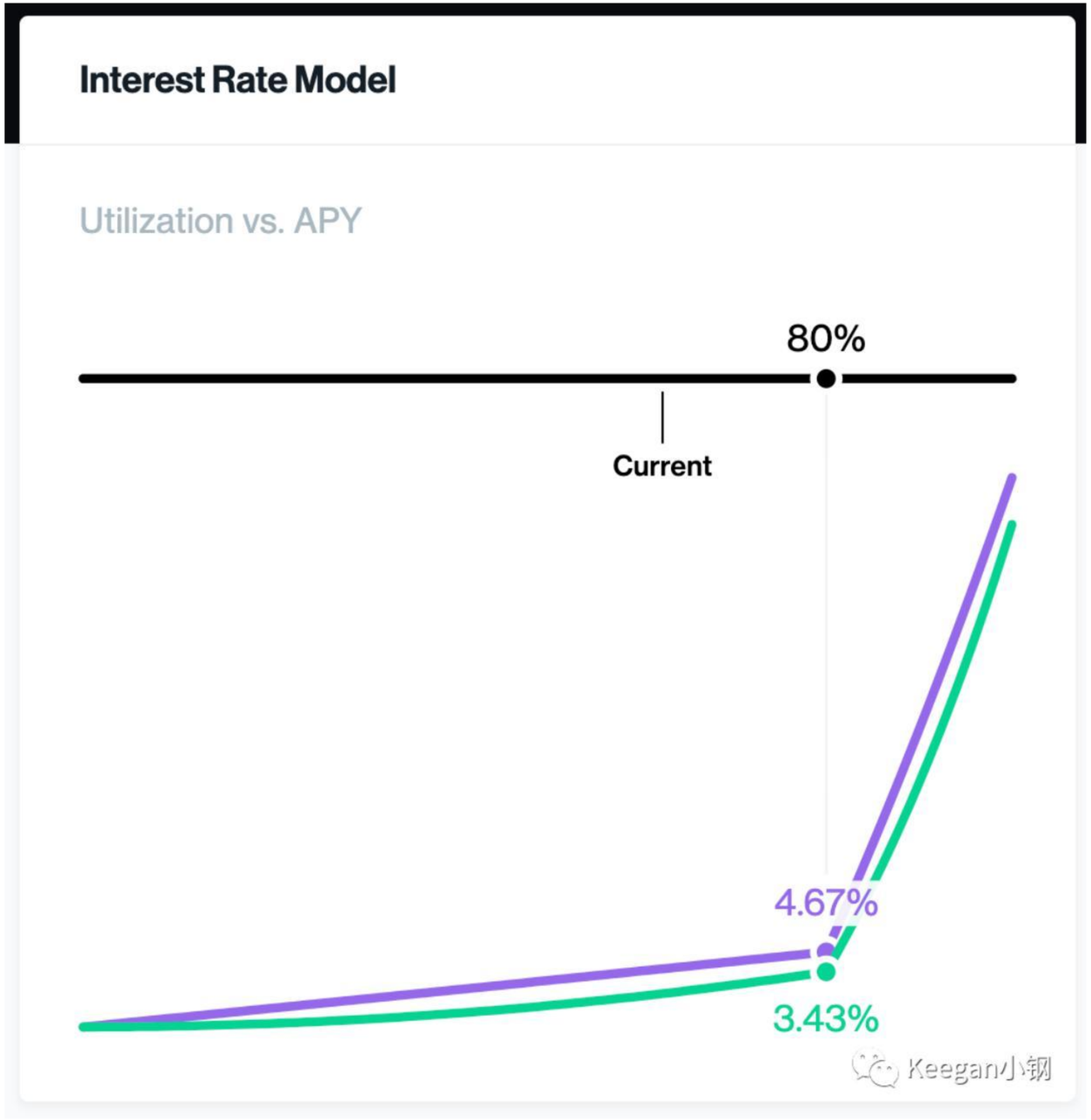
直线型利率模型

- 借款利率曲线为一条直线
- 借款利率：
  - y(borrowRate) = k * x + b
- 存款利率：
  - supplyRate = x * borrowRate * (1 - reserveFactor)



拐点型利率模型

- 借款利率曲线为两段直线
- 第一段的借款利率：
  - y1 = k1 * x + b
- 第二段的借款利率：
  - y2 = k2 * (x - p) + (k1 * p + b)
- 存款利率：
  - supplyRate = x * borrowRate * (1 - reserveFactor)



利率机制

区块利率

- 随时间推移，利率会随供求关系变化而调整
- 将年利率转为区块利率来计算
- 通过利率指数（ Interest Rate Index ）掌握每次利率变化
  - index(a,n) = index(a,n-1) * (1 + borrowRate * blockDelta)
- 也存储每个用户最后一次计息时的余额和利率指数

代码解析

合约代码

https://github.com/compound-finance/compound-protocol

- WhitePaperInterestRateModel
- BaseJumpRateModelV2
- CToken
- Comptroller

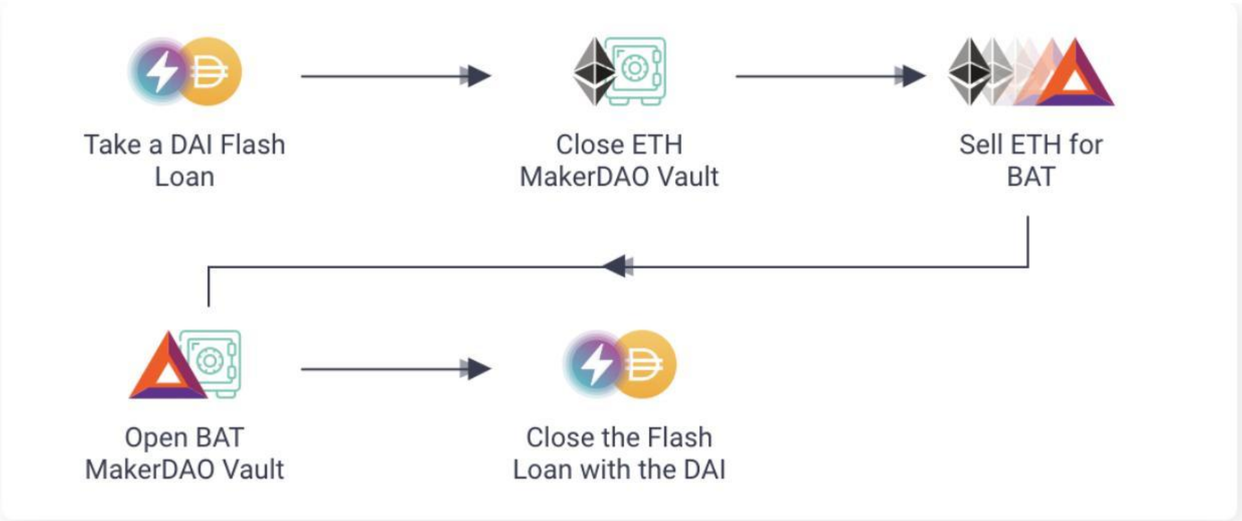
Aave闪电贷

https://docs.aave.com/faq/flash-loans

闪电贷原理

无抵押贷款

- 无抵押贷款的DeFi产品
- 需在一个交易内完成借款和还款



Flash Loan use case: Collateral swap of a MakerDAO Vault

执行流程

概要流程

- 调用 Pool 合约的 flashLoanSimple() 或 flashLoan()
- Pool 合约将所借资产转到调用者指定的 receiver 合约地址
- Pool 合约调用 receiver 合约的 executeOperation()
- receiver 合约的 executeOperation() 执行自己的逻辑
- receiver 合约的 executeOperation() 授权给 Pool 合约所借金额 + 手续费
- Pool 合约调用 safeTransferFrom() 从 receiver 转账过来
- 处理还款后续事宜

应用示例

套利

- 假设某一个代币在两个 DEX 之间存在有利可图的价格差，就可利用闪电贷实现套利
- 核心在于实现接收闪电贷资产的合约，需实现 IFlashLoanSimpleReceiver.sol 或 IFlashLoanReceiver.sol 接口
- 可直接继承自抽象合约 FlashLoanSimpleReceiverBase 或 FlashLoanReceiverBase
- 核心逻辑在于实现 executeOperation() 函数

闪电贷攻击

攻击案例

- 2020年2月16日，bZx 遭受闪电贷攻击，15秒内被套利36万美元ETH。
- 两天后，即2月18日， bZx再次被闪电贷攻击，攻击者或获利2388个ETH。
- 10 月 26 日，DeFi 项目 Harvest Finance 遭到闪电贷攻击 ,造成了约 2400 万美元的损失。
- 11 月 14 日，Value DeFi 协议遭到闪电贷攻击 ,最终导致超过 700 万美元的损失。
- Akropolis 、Cheese Bank 和 Origin Protocol 等 DeFi 协议 ,也同样接连遭到闪电贷攻击，均为百万美元级别以上

如何避免闪电贷攻击

安全攻略

- 需要用到外部价格做为条件判断时，如清算，使用安全的价格预言机，如 Chainlink、 Uniswap TWAP。
- 某些场景可限制在同个区块内的多次操作，比如衍生品 DEX ，可以限制在同个区块内同时开平仓。
- 某些场景可添加全局的交易滑点保护，比如当前区块内成交价格不能超过之前区块最后一口价格的 5% 。


Thanks
AMA
Keegan / 2020年3月24日