Defi 🚀

传统金融机构

银行：
作用：通过提供价值转移（存、取、转账），提高信贷额度（贷款）等服务，使资金能在世界流转

缺点：
容易受到human-related风险

Defi优化了：
1. 支付和清算系统（汇款）
2. 可获取性
3. 中心化和透明度

1.支付与清算系统

银行：
1. 时间久
2. 手续费高
3. 可能涉及记明文件、反洗钱、隐私等法律

加密货币：
1. 交易速度快
2. 手续费低
3. 交易无条件处理

2.可获取性

银行：
1. 验证流程冗长
2. 某国地区准申请

Defi：
1. 流程简单
2. 无国界、无障碍、无审查

3.中心化&透明度

中心化金融的缺点：
1. 权利、资金集中
2. 投资者无法充分了解金融机构的运作

Defi是什么

1.Defi是一场能让用户无需依靠中心化实体的金融服务活动
2.Dapp提供这些金融服务
3.大部分应用部署在以太坊平台上
4.用户通常需要将抵押品锁定在智能合约中
5.Dapp中锁定抵押品基计价值被称为锁定总价值

Defi生态

Defi的主要类别

稳定币

去中心化借贷的一些优势：
1.取消信用评级
2.无需抵押品
3.无需银行账号
4.通过抵押数字资产获得贷款
5.把数字资产注入借贷池获得收益

借贷

交易所

中心化交易所：
Coinbase、Binance

- 交易资产的中介、托管方
- 交易所用户不能完全控制资产
- 交易所可能被攻击或无法偿还债务

去中心化交易所　用户无需存入资产

衍生品

衍生品是一种价值来源于股票、商品、货币、指数、债券或利率等其它标的资产的合约

基金管理

基金管理是监管你的资产并管理其现金流以产生投资回报的过程

传统基金管理
- 主动型：管理团队/经理决策
- 被动型：指数决定

Defi　被动型

彩票

1.Defi的彩票可将资金次的托管转移到以太坊的自能合约上。
2.比如：将参与者资金汇集到一起，再将汇集的资金投资到Defi的贷款Dapp中。以设定的时间间隔将利息交给中奖者。选中中奖者后，所有购买者将拿回下注的资金

支付

进行无需信任、去中心化的转账

保险

所有智能合约中锁定的代币都容易受到智能合约漏洞的影响，永远无法知道该智能合约是否真的安全

Defi的运行原理

1.为缓和加密货币的剧烈波动，锚定美元等稳定资产的被创造出来。
2.比如USDT，每枚USDT在其发行机构账户上都有1美元作为背书
3.去中心化稳定币是通过超额抵押（overcollateralization）的方法以去中心化形式创建，完全在去中心化基本上运行，由去中心化自治组织管理。其准备金可以由任何人公开审计。
4.稳定币是稳定的价值存储手段。

Defi如何进行系统自治

治理

发行DAI的目的

3种可能的场景

现在需要资金，并拥有一种你相信未来会升值的加密资产
- 将加密资产存入Maker金库
- 通过发行Dai立即获得资金

现在需要资金，但不想因出售加密资产触发纳税事件的风险（？）
- 通过发行Dai来提取贷款

投资杠杆

如何获得一些Dai

铸造Dai

抵押率Collateral Ratio
- 可铸造的Dai数量取决于抵押率
  - ETH抵押率 = 150%
  - BAT抵押率 = 150%

要铸造100USD的Dai，需要至少抵押价值150美元的ETH或BAT

稳定费Stability Fee　借款人就Maker金库债务本金外所要支付的利率

Dai存款利率Dai Savings Rate（DSR）　持有Dai一段时间后所获得的利息

预留空间保证抵押率在150%以上，以防止金库被清算和被收取13%的清算处罚

交易Dai　二级市场交易

黑天鹅事件

可能造成严重后果的一类不可预测极端事件

去中心化稳定币

为缓解加密货币价格的波动，价格锚定稳定资产被创造出来

稳定币的类型

法币抵押型

储备金储存在金融机构中

用户必须信任该类型币作为一个实体，确实拥有其声称的准备金数额

加密货币抵押型

该类型币的价值，是由一个DAO表决的协议和智能合约来实现与1美元的锚定

在任何时间，用于生成该类型币的抵押品都可以被用户验证

Maker

Maker是一个运行在以太坊区块链上的智能合约平台

Maker拥有3种代币

Sai
- 单抵押Dai
- 仅由ETH作为抵押品背书

Dai
- 多抵押Dai
- 目前由ETH、BAT作为抵押品背书，并计划以后增加其他类型资产作为抵押品

Maker　Maker的治理代币

Sai和Dai的区别

单抵押 Dai = 遗留 Dai = Sai

SAI将被淘汰并且不再得到Maker的支持

多抵押 Dai = 新型 Dai = Dai

如何进行系统自治

MKR持有者在该DAO组织中拥有与自己持有MKR代币数量成正比的投票权

MKR在DAO中的用途

MKR持有者可以对治理Maker协议的参数进行投票

Dai稳定币生态中3个关键参数

为什么使用Maker

稳定币之间的核心区别在于他们的协议

Maker完全运行在分布式账本上
- 安全
- 不可篡改
- 透明性

天生具有区块链特性

Maker的基础设施通过基于实时信息且全面的风险协议和机制，加强了系统的安全性

以太坊钱包

1.链接区块链网络的用户友好接口
2.管理私钥
3.接收、储存、发送加密货币

钱包分类

托管：
将控制权交给第三方，风险在第三方

非托管：
自己控制钱包，风险在自身

钱包选择

移动端用户：Argent

Argent卫士
- 可验证使用者身份的人
- 可验证使用者身份的设备
- 可验证使用者身份第三方服务

日交易限额

免费交易（待考证）

桌面端：MetaMask

Metamask是浏览器扩展程序

Metamask可以保存以太币和ERC20代币

Metamask可作为与以太坊网络中的Dapps交互的桥梁

类似Metamask的交互桥梁免去了必须下载整个庞大的以太坊区块链节点的工作。

Metamask通过注浏览器注入web3.js的库让用户轻松与以太坊网络进行交互

去中心化层：以太坊

以太坊：面向去中心化应用的全球开源平台

大部分Dapps搭建在以太坊区块链上

开发人员可以在以太坊上编写智能合约。
智能合约通过一套标准对数字价值（digital value）进行控制

世界上任何地方可以访问

软件工程师编写的智能合约是这些Dapps的组件，这些智能合约被部署到以太坊网络，并在网络中全天候24小时运行，该网络会持续维护数字价值账本，并跟踪其最新的状态。

智能合约：可编程合约

- 允许交易双方设置交易条件
- 交易的执行无需信任第三方
- 遵循"if this, then that"原则
- 多个智能合约组成Dapp

Ether(ETH)：以太坊区块链的原生数字货币

基于当前币价购买物品、服务

支付智能合约和Dapp在以太坊上运行的费用（在以太坊上执行只能合约，需要支付Gas fee）

以太坊区块链记录交易，保证交易的不可改变性
以太币增值潜力为以太坊自身链的价值储存、储备货币

Gas

Gas指的是执行某项操作或某个智能合约 所需计算资源的度量单位（the unit of measure on the amount of computational effort）

Gas fee可以手动设置

Gas fee高，优先被验证，验证通过即被添加到区块链中

Gas fee低，会被排入队列，需要一段时间才能进行Bi

Gas fee的单位为gwei (1gwei = 0.000000001ETH)

Gas fee = 需支付的Gas量 * Gas的市场价价

完全以ETH支付

Gas fee依赖于当前网络需求

网络计算资源有限
- 更多的人在以太坊区块链上交互：Gas fee上涨
- 网络未被充分利用：Gas fee降低

Dapps

Dapps是区块链与用户交互的接口

优势

不变性Immutability
一旦信息保存在区块链上，不能被任何人更改

防篡改Tamper-proof
发布在区块链上的智能合约，不能在其他区块链参与者不知情的情况下被篡改

透明性Transparent
智能合约驱动的Dapp是公开可审计的

可用性Availability
只要以太坊网络保持活性，在其之上搭建的Dapp将保持活性和可用性

劣势

不变性Immutability
人为错误是不可避免的，而不可变的智能合约有可能会将错误固化

透明性Transparent
源码能被黑客查看

可扩展性Scalability
Dapp的带宽受制于所在区块

以太坊的其他用处

创建去中心化自治组织（DAO）

完全自治，不由个体管理，只通过代码管理

DAO代码基于智能合约运行

透明

DAO管理决策通过代币投票决定

作为平台发行其他加密货币

ERC-20：
可互换代币，意味着代币间是可互换的并具有相同的价值

ERC-721：
不可互换代币，意味着代币是唯一的且不可互换的

其定义了在以太坊上发行代币的规则和标准