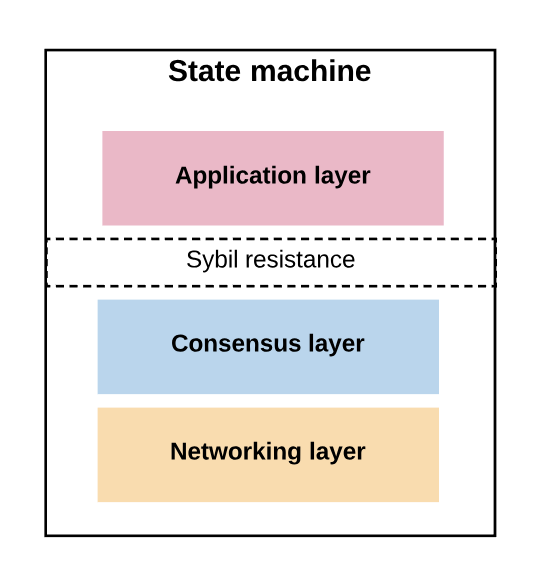
KAWA 调研报告

## 一、COSMOS

因为KAWA是建立在COSMOS上的，先简单介绍一下COSMOS。

### **架构**

COSMOS是Tendermint团队开发的，他们将区块链理解为“状态复制机”，然后将区块链架构从上到下分为三层：**应用层，共识层，网络层**。另外在共识层之上还有一层“**抗女巫攻击层**”，如果没有这一层，攻击者可以通过创建许多假身份来篡改状态，从而获得与其投入不成比例的影响或收益，狭义的POW和POS本质上都是属于这一层。整个架构如下图所示。



COSMOS的最终目的是建立区块链网络。为了方便用户，COSMOS提供了很多工具，如**Tendermint BFT，COSMOS SDK，IBC**等。

1. Tendermint BFT提供了网络层和共识层，使用它用户可以很方便的搭建自己的链，而不用从头开发自己的网络层和共识；
2. COSMOS SDK是为了方便用户开发应用程序，它内部提供了很多应用的模块，用户可以利用这些模块写出自己的上层应用；
3. IBC全称是Inter-Blockchain Communication Protocol，目的是通过协议将各个区块链连接起来。它将运行在COSMOS上的区块链分为两类：**Hubs** 和 **Zones**，Zones就是各个独立的链，Hubs负责连接起Zones。另外还有对应于Bitcoin、Ethereum等非确定性共识区块链的Peg Zone。这里面还有很多的细节，很多功能COSMOS还在开发中。

COSMOS上运行的第一个Hub是“COSMOS Hub”，在去年（2019年3月13日）主网上线，它的token叫做ATOM。下面介绍它的POS机制。

### **POS**

共识机制和经济模型是在一起的，两者之间有紧密的关系，这里就一起介绍。但总的来说，底层是Tendermint BFT共识，上层是POS机制，放在一起统称为“POS共识协议”。下面为了方便介绍，统一用“钱”来称呼ATOM，用人的形式来称呼链里的各个角色。

COSMOS Hub每6s出一个块。一个出块的总体流程是： 选举leader打包交易，传播给所有的其他节点；其他的人作为validator验证块；如果块合入了链，那么**leader** 和 **validator**都会得到奖励，leader的会多一些。

这里面最关键的就是leader选举算法。COSMOS Hub实现了一个**随机选择算法**，能够兼顾优先性和公平性。优先性就是谁拥有的ATOM数量多，那么这个人被选举为leader 的机会就大；公平性是指不管某个人持有的ATOM数量有多么的少，他都有机会成为leader。

POS共识本身有个问题，就是容易受到“无利益攻击”（Nothing at Stake Attack）（见参考4）。为了解决这个问题，COSMOS Hub使用了**stake**（质押）和**slashing**（惩罚）机制。每个参与共识的人都要抵押钱，称为stake；如果作恶了，这些钱就被收走了，称为slashing。

为了链的安全，应该吸引人们参与到链的验证当中去。这就引出了新的概念：delegator和bonding，以及通胀机制。**Delegator**翻译过来就是“委托人”，如果他不参与到区块链的验证当中去，他可以把钱借给validator，这样子不管这个validator是出块，还是做验证，都能得到收益，而他（delegator）也可以得到一部分费用。Delegator把钱借给validator的过程就称为**bonding**。上面是鼓励大家参与验证，还有一条是惩罚那些不积极参与验证的，也就是**通货膨胀机制**：当 ATOM 的质押数量小于 2/3 的 ATOM 流通总量，ATOM 的价值每年都会下降，最高可下降 20%。通过这个系统，只持有通证而不去委托对于 ATOM 持有者没有一点优势，相反，将通证委托给验证人有很大可能性会增加通证总量来扩大他们的投资价值。

另外，如果delegator投钱给的那个validator作恶，不仅validator的钱会被slashing掉，delegator也会损失一部分钱。

关于COSMOS Hub的经济模型，我有一些疑惑：

1. COSMOS Hub鼓励大家去stake，这样不就降低流通量了吗？对整个经济生态是否有益？
2. delegator的选择机制是否会造成马太效应？假如大家都投给同一个人，那这个人成为leader 的几率就会大，然后delegator的收益是否会变大呢？当然了，人数一多，平均下来分的就少了，这里面应该会有个数学模型可以分析怎么样收益最大，这样一来，那个随机选择算法是否还能够很好的起作用了呢？

这个可以以后再看。

## 二、DeFi & CDP

KAWA是个DeFi平台，这里简单介绍一下DeFi是什么和里面的一个核心概念CDP。

### **1. DeFi**

DeFi是2019年区块链领域最火热的话题之一，网上很多资料将DeFi理解为“去中心化借贷”，其实DeFi有更广泛的意思，它的全称是“Decentralized Finance”，“**去中心化金融**”，也被称为“开发金融”（Open Finance），包括货币发行、货币交易、借贷、资产交易、投融资等。它是在加密货币的基础上引申出了金融的概念，它可以将加密货币的概念包含进去，可以将加密货币称为DeFi的第一个阶段，而近两年发展迅猛的“去中心化借贷”将DeFi带入第二个节点，以后可能会有更多的新发展。下图是DeFi于传统金融等的对比。



去中心化借贷是指通过去中心借贷协议匹配借方与贷方，再抵质押确认后即时划转资产、完成借贷行为。下图是抵押借贷流程。

去中心化借贷有三种模式：P2P撮合模式，稳定币模式，流动池交易模式。

1. P2P撮合模式

Dharma 和 dYdX 都是撮合借方和贷方的点对点协议。因此，基于这两个协议的贷款和借款数量是相等的。

1. 稳定币模式

典型是 MakerDAO，没有贷方只有借方，且唯一可借入的资产是 DAI。借款人通过抵押数字资产（现为 ETH）借入新创造的 DAI。DAI 是MakerDAO 平台发行的、与美元挂钩的稳定币。

1. 流动池模式

典型是Compound，借方和贷方通过流动性交易池进行交易，而不是与交易对手进行匹配。



### **2. CDP**

抵押过程中有一个关键的概念：CDP。CDP的全称是Collateralized Debt Position，一般翻译为“抵押债仓”。用最简单的话来说，就是你将数字资产放入CDP中，然后得到贷款；等你还上贷款之后，能够从CDP中取出抵押的资产，然后关闭CDP。当然，这个过程中有很多细节。

目前最成熟的是MakerDAO，下面以它为例介绍CDP的一些基本用法和细节。

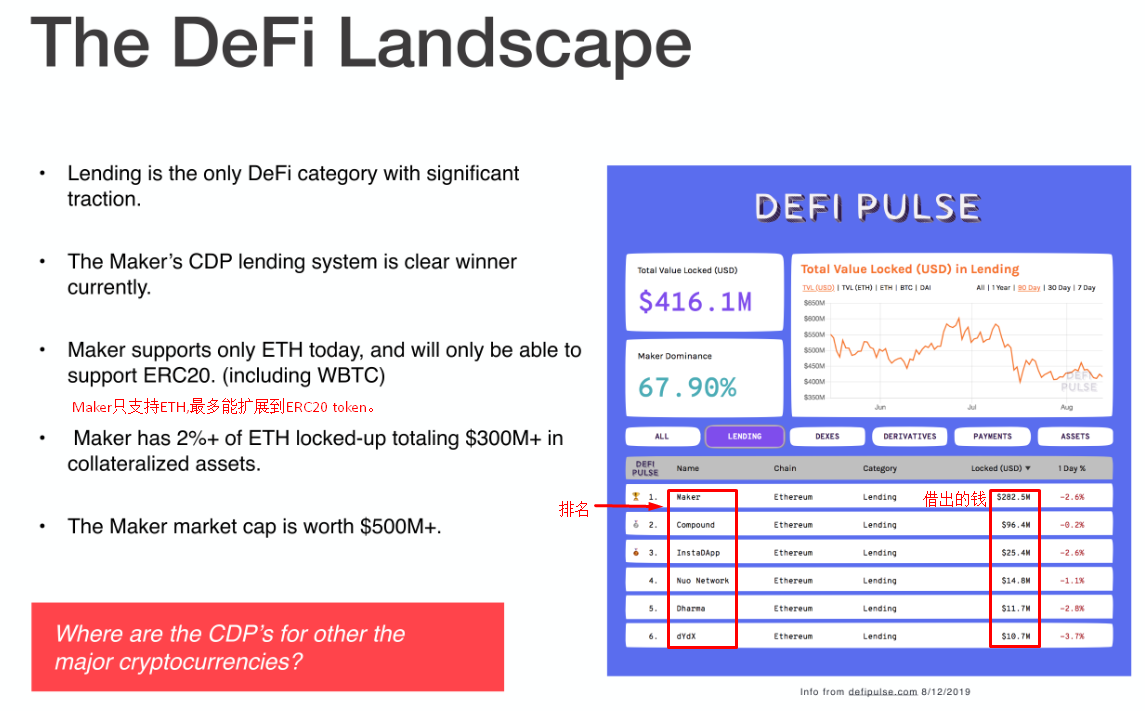
1. MakerDAO 抵押债仓（CDP）是一种运行在以太坊区块链上的**智能合约**管理的贷款方式。
2. CDP 是 **Dai 稳定系统**的核心部分，用户通过抵押品借出**生成 Dai**，该系统将一直保管抵押品直到贷款人偿还借出的 Dai，偿还债务时**销毁 Dai**。Dai 生成之后，CDP 用户可以用它做任何想做的事。
3. 每个 CDP 都是**超额抵押**，即 CDP 中的抵押品价值高于债务数额。**抵押比率**是用户 CDP 中抵押品价值与所借出的 Dai 之间的比率。
4. CDP 的抵押品**没有上限**。
5. CDP 是**无需许可**的，任何人都可以创建和使用。任何想要生成 Dai 的用户都可将 ETH 存入 CDP。
6. CDP 要**收费**。CDP 持有者需要为他们借出的债务支付**稳定费率**。
7. 只要 CDP 持有者保证**最小抵押比率**（**清算比率**），他们就可以**自由地借出或存入**多余抵押品。
8. 如果 CDP 抵押不足，就会被进行**清算**，系统将自动接管其资产，然后向市场打折出售以弥补未偿债务。同时会有清算罚金。
9. **清算并不会关闭** CDP。用户可以在偿还全部债务和相关费用后**关闭**他们的 CDP。
10. 持有 CDP 本身是**有风险**的。
11. 使用 CDP 有**好处。**
12. 可以不创建 CDP，直接在交易所购买 Dai。

三、KAWA

### **1. 简介**

KAWA是建立在COSMOS上一个DeFi平台，本质是COSMOS网络中的一个Zone，也就是一条区块链 + 应用。这个应用就是DeFi平台。

KAWA对标Ethereum上的MakerDAO。目前去中心化借贷是比较火热的领域，MakerDAO是其中的领跑者（见下图），可以看出市场还是挺大的。



但MakeDAO只能支持ETH，最多扩展到ERC20 token，而KAWA的目标是依托于COSMOS平台，支持很多主流币种，如BTC, XRP, BNB, ATOM；另外的好处就是KAWA使用的是COSMOS的Tendermint共识，性能要强于Ethereum的POW共识。

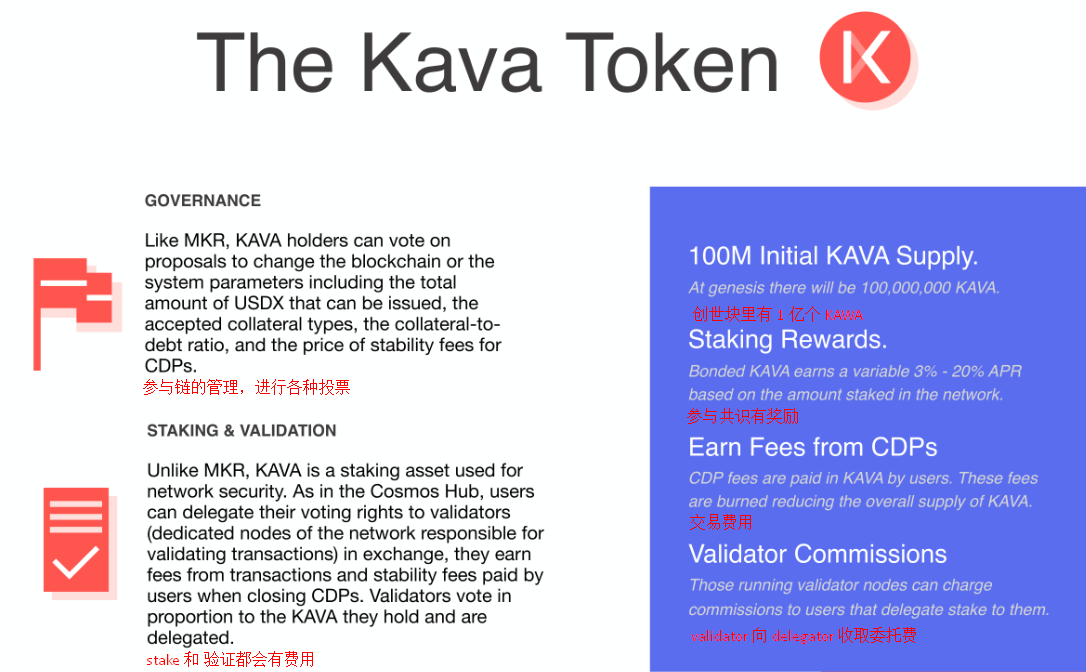
目前KAWA的很多功能还在开发中。去年（2019年11月5号）上过主网，但是出现了分叉，发现了潜在双重签名攻击，后来忙于其他项目，就一直推迟，目前最新消息是**今年4月28日重新上主网**。

另外，可能是因为忙于开发，KAWA**几乎没有技术说明文档**，无论是官网还是Github上，白皮书（<https://docsend.com/view/gwbwpc3>）也是非常简单。资料是通过新闻报道、Blog、Medium、Telegram群中获得。

所以下面的描述有可能跟真正主网上线的功能不一致。

### **2. 经济模型和共识机制**

总的来说：在底层，KAWA的共识和COSMOS Hub基本一致，是Tendermint BFT + POS的形式，token 的名称也是KAWA，是用来管理和维护区块链的运行； 在上层，跟MakerDAO流程很像，可以将KAWA放入CDP中，贷款出USDX，然后就可以随意使用这些贷款。USDX是一种跟美元挂钩的稳定币。



1. **创世块**里生成了1亿个KAWA。之前是在币安上面IEO了。
2. 跟COSMOS Hub一样，有**validator和delegator**：Validator通过参与共识获取奖励；delegator将自己手里的token委托给validator，来获取一些收益。
3. 每笔交易都有费用，这些**交易费**会分给共识参与者，包括validator 和 delegator
4. KAWA有**通胀机制**：
   1. 块奖励。

每生成一个块，都有产生新的KAWA token，分给validator 和 delegator。这个产生的token 的数量是变化的，依赖于共识中质押的token 的占比。这样子能够鼓励大家参与共识中来，从而保证链的安全和稳定。**通货膨胀率**最开始时是7%，如果参与共识的人少，通胀率就会一直上升，最大可到20%，如果参与共识的人超过了2/3，通胀率就会下降，最小是3%。这些比率都是按年计算的。

* 1. CDP清算时挖出新的KAWA

如果有CDP被清算了，即资不抵债，就会有新的KAWA被挖出，直到能够偿还债务。

1. KAWA有**通缩机制**：用户抵押贷款，需要在结束时缴纳一定的费用。这个费用是使用KAWA支付的，这笔钱会被**销毁**掉。最开始时这个费率是固定的，一年5%，举个例子，如果第一年关闭的CDP值100个USDX，那么就有价值5个USDX的KAWA被销毁掉。
2. **委托费用**：validator可以向delegator收取委托费用。这涉及一些具体的策略，validator可以灵活的使用各种策略来吸引delegator将钱托付给自己。默认模式是设置一个统一的收费比例：就是出块奖励和交易费奖励的收费比例都一样。
3. 在管理上，共识参与者可以进行很多种**投票**，来修改上面所说的各种关键参数。

### **CDP流程**

KAWA的CDP流程包括抵押流程、偿还流程、清算流程：

1. 抵押流程：

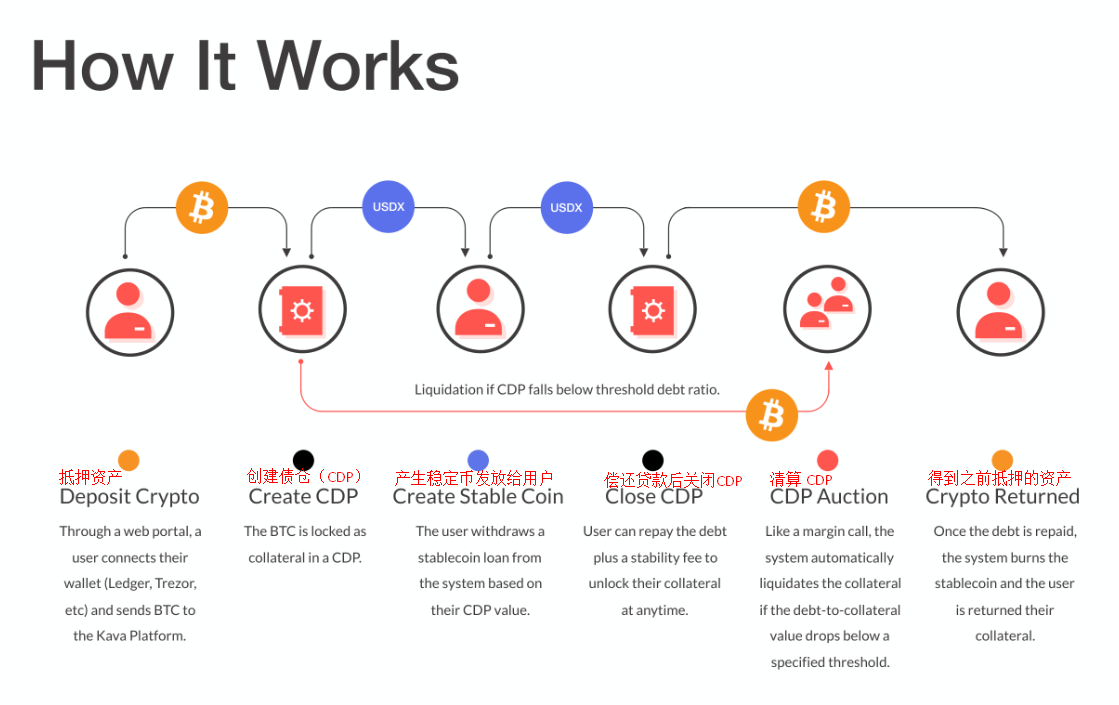
用户拿出资产 -> 创建CDP，将资产锁定进去 -> CDP系统会发方USDX给用户-> 用户可以拿这些USDX做任意想做的事情

1. 偿还流程：

用户偿还借出的USDX，外加一定的费用 -> 可以选择关闭CDP –> CDP 系统会将之前用户抵押的资产返还给用户

1. 清算流程：

如果CDP系统发现CDP里面抵押的资产已经贬值到最小比率，会自动启动清算流程，对CDP进行清算，包括将里面的资产卖出，挖出一些新的KAWA币等。



### TestNet

KAWA没有现成的TestNet供使用，因为时间关系，没有来得及部署。具体的部署步骤见参考9.

如果时间充足的话，还可以体验一下使用Tendermint BFT 和 COSMOS SDK搭建一条自己的链。

四、参考

1. COSMOS官网：

介绍 <https://cosmos.network/intro>

SDK <https://cosmos.network/developers>

1. COSMOS原理介绍

<https://www.preethikasireddy.com/post/how-does-cosmos-work-how-does-it-compare-to-bitcoin-and-ethereum-part-1>

<https://www.preethikasireddy.com/post/how-does-cosmos-work-how-does-it-compare-to-bitcoin-and-ethereum-part-2>

1. COSMOS Hub 和POS原理

官网：<https://hub.cosmos.network/master/hub-overview/overview.html>

POS原理:<https://medium.com/the-cosmos-guardian/proof-of-stake-on-cosmos-network-explained-to-my-dog-f7367297e5ae>

1. Nothing at stack

<https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027>

1. DeFi介绍

<https://www.chainnews.com/articles/895348768931.htm>

1. CDP

<https://defipulse.com/blog/what-is-a-cdp/>

<https://community-development.makerdao.com/makerdao-scd-faqs/zh/cdp>

<https://www.jinse.com/blockchain/496231.html>

1. KAWA

官网：<https://www.kava.io/>

白皮书：<https://docsend.com/view/gwbwpc3>

1. KAWA token economics

<https://medium.com/kava-labs/kava-token-economics-3df1a00efb27>

1. KAWA testnet

<https://medium.com/kava-labs/guide-to-joining-the-kava-testnet-9e697d381e07>