北大汇丰

PHBS FINANCIAL FRONTIER DIALOGUE

金融前沿对话

2021 年第 18 期　总第 104 期

PHBS HFRI
北京大学汇丰金融研究院

北京大学汇丰金融研究院简介

北京大学汇丰金融研究院（The HSBC Financial Research Institute at Peking University，缩写HFRI）成立于2008年12月，研究院接受汇丰银行慈善基金会资助，致力于促进金融学术研究、金融市场运行、金融机构监管、金融政策决策之间的交流互动；立足粤港澳大湾区，以全球视野，构建开放的金融专业交流平台，使金融教学与金融研究相互带动，通过编辑出版专业刊物、发布专业研究报告、举办专业讲座、组织前沿学术会议等多种形式，为区域金融发展和国家金融决策提供积极的智力支持，努力将北京大学汇丰金融研究院打造成为聚焦市场前沿的金融专业智库。

北京大学汇丰金融研究院院长为北京大学校务委员会副主任、北京大学汇丰商学院院长海闻教授，执行院长为中国银行业协会首席经济学家、中国宏观经济学会副会长巴曙松教授。

Defi 创新趋势

【对话主持】

巴曙松（北京大学汇丰金融研究院执行院长、中国银行业协会首席经济学家、中国宏观经济学会副会长）

【特邀嘉宾】

邱明（罗汉堂资深专家）

一、Defi 的定义

与我们通常比较熟悉的金融机构不同的是，Defi 主要是指基于区块链的金融服务。首先，它需要有一个开源的公链作为底层价值体系。现在用得最多的还是以太坊，但是也有其他的公链可以用作底层价值网络体系。在公链价值网络体系之上，垂直的金融功能，如稳定币、去中心化的交易所、资产管理、借贷、保险以及资产的通证化等，就可以被开发出来。这种开发是基于一种可审核的开源智能合约方式，而不是像传统金融基于一整套账户体系，然后通过金融机构本身的软件系统功能来实现金融服务。

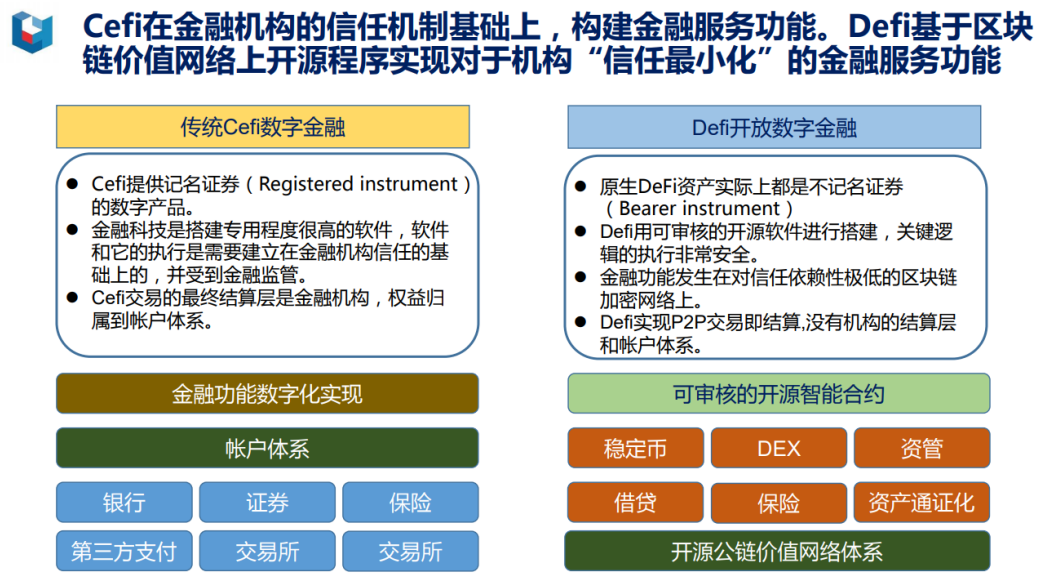
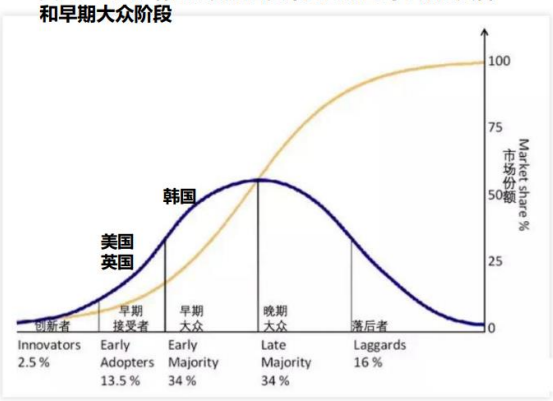


图 1

我们可以看到，一方面可以把 Defi 归类为这种不记名证券，另一方面也可以把它归为不像传统金融机构那样对主体有非常严格的 KYC、对金融用户或者金融消费者有非常严格确认的一种账户体系。所以 Defi 在监管和保护金融消费者等方面其实还是有很多的开放性问题。

如图 2 所示，根据一些数据的综合分析，我们现在基本上可以判断，在全球范围之内持有加密货币的人可能达到一个亿，也可能会略少一点。由于他们是通过这种中心化的交易所来持有加密货币的，所以这里我们也可以稍微计算一下，它在互联网用户的渗透率大概接近 2%，在全球人口的渗透率大概为 1.2%。

推算全球持有加密货币权益的人数约1亿，在互联网用户中渗透率1.9%，全球人口渗透率1.2%



数据

- 谷歌扩展数据显示，3月22日，MetaMask（小狐狸钱包）下载量突破200万
- 截至2020年12月31日，Coinbase认证用户总数达4300万，较2019年底增长34.4%；截止3月31日，认证用户已经达到5600万，2021年前3个月增长了30%，**推算美国17%人口投资加密货币**
- 英国金融行为监管局（FCA）去年发布的报告Cryptoassets Consumer Research 估算，截止2019年底，3.86%的英国人口持有加密资产，**推算英国5%人口投资加密货币**
- 截至2018年1月，韩国使用数字货币服务的用户总量达到509万，占人口9.8%，**推算韩国20%人口投资加密货币**
- 全世界总人口78亿，全球互联网总人口是50.53亿。**推算目前全球总持币人数是1个亿**，那么加密货币在互联网用户中的渗透率为1.9%，在全球人口的渗透率为1.2%。

图 2

基于对区块链真实用户的分析，我们基本上可以判断出来，持有加密货币的人数大概在 500 万左右。具体计算的过程如图 3，比如比特币和以太坊余额多于 0.01 个的真正的地址数总计将近 2000 万，而 Defi 的独立的地址数大概是 160 万，所以我们可以大致的推断出来区块链上的用户是 500 万，而 Defi 的真正用户大概是在 10 万到 30 万，可能是会偏近 10 万这个下限一点。

推算区块链上独立用户约500万，Defi的使用者大约在10万到30万之间，

比特币余额>0.01的地址数889万

- BTC总地址8.03亿，非零地址3677万，仅占4.58%
- 比特币采用的特殊的UTXO模型，这些余额非零的地址中可能存在大量找零地址。找零地址同样可能因为无法支付交易手续费而成为“沉默”地址

以太坊余额>0.01的地址数1322万

- ETH总地址1.06亿，非零地址5588万,比2017年增长123倍
- 以太坊上的平均交易手续费大约为0.01ETH，余额低于0.01 ETH的地址也可被视为“沉默”地址

Defi独立地址167万，平均日活地址4.1万

- 假设每5个独立地址对应1个独立用户，两条公链的用户重叠率为30%时，预计比特币和以太坊的用户总数大约为388.91万人
- 按照BTC, ETH市值占比80%推论，预计区块链链上用户的总数大约为500万人

图 3

如果我们再分析得细一点，如图 4，对于公链每天的活跃地址数以及 Defi 的日活数的分析可以看到，虽然从 2020 年以来，Defi 非常火热，但是真正的平均每一天的日活地址，除了 Uniswap、Synthetix 和 SushiSwap 这三个应用之外，其他真正的日活地址都少于 1000 个。也就是说遵循不同 Defi 协议的玩家的数量范围在几百到几千这样的区间内。

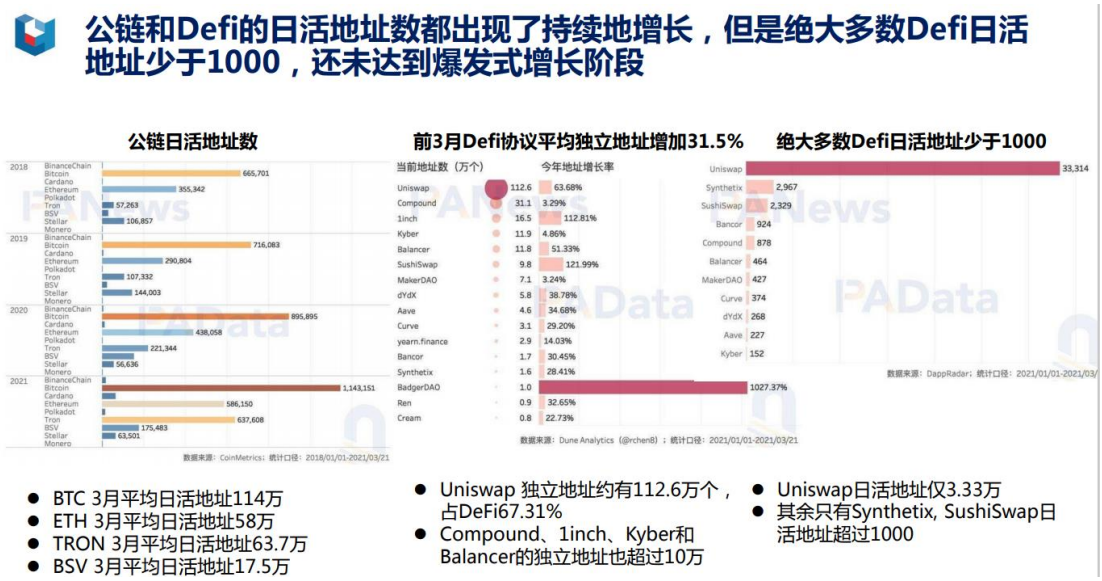


图 4

图 5 列出了一些基于区块链的中心化的应用。例如，Coinbase 首次 IPO 上市，上市首天其市值保持在了 850 亿美元左右。对于一个 2012 年才刚刚成立的公司来讲，这个成绩应该说是非常好。除此之外，还有 Kraken，也是加密交易所，也有上市的打算。同时，Robinhood，作为线上的 broker dealer，在加密货币的交易方面也有比较大的量。另外，美国的一些支付公司，也有通过比特币和以太坊支付的功能。

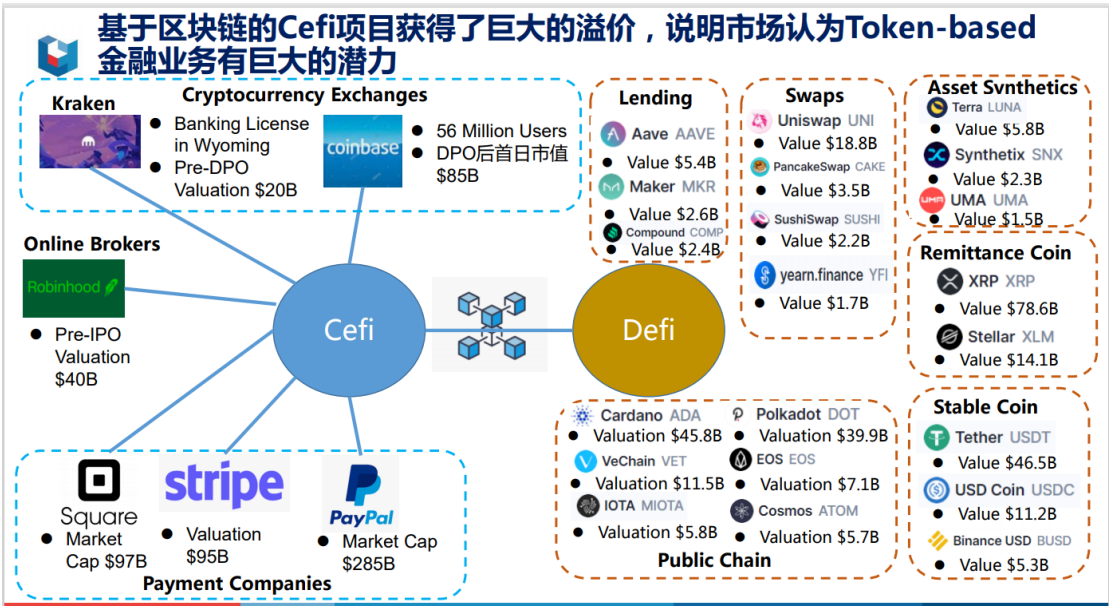


图 5

如图 6，当我们来回顾基于以太坊的 Defi 的发展历程，可以看到很多金融的基本功能。比如，从最基础的 2017 年 12 月份的 MakerDAO，即一个算法稳定币的协议产生；到可以进行存和贷的第一代去中心化银行的服务，也就是 Compound；再到去中心化的交易所 Uniswap，这时候已经到了 2018 年 10 月份；然后再到线上和线下或者是链上和链下的资产混合 Synthetix，在 2018 年 11 月份出现；后来又有一些跨链的资产，比如 token 资产的互相转移。在 2019 年 7 月份有一个非常重要的聚源集 ChainLink。目前很多时候区块链还需要从互联网上获得信息，而这些信息要通过智能合约转换成其他的可以使用的智能合约，这个就是 2019 年 7 月份的 ChainLink。然后在 2020 年 1 月份，所谓的第二代去中心化银行 AAVE 开始出现。从 2020 年下半年一直到现在，在 Defi 领域一个非常重要的趋势或者发展，就是 Yield Farming，即收益农耕。应该说是由于 Yield Farming，一方面有需求，

一方面有供给，造成的一个根本变化就是持有一些有在 Defi 使用的 token 时，可以产生利息。从这个角度上来讲，它已经发生了一个质的改变，也就是说一部分的加密货币开始变成一种真正金融意义上的资产。

图 6

在区块链领域，从比特币到以太坊，这些都是属于非稳定币，他们和法币的价值是在不断波动中。那么，要实现各种金融的功能，它其实是需要和法币有一个锚定。到目前为止，稳定币主要是以 1：1 比例的和美元挂钩。当然也有其他一些规模比较小的稳定币，跟新加坡元、日元以及英镑挂钩，但是最主要的还是和美元的 1：1 挂钩。它本身的实现方式非常有意思：一种是我们非常习惯的，比如说找一个信誉非常好的托管银行，像 BNY Mellon，这是最大的 custodian bank，它可以持有美元来作为储备的资金，同时作为稳定币的发币方，它可以发行这种数字稳定币，这里我们讲的还是私人的稳定币，还不是最

近美联储谈到的数字美元；另一种是采用去中心化的方式来实现稳定币。

图 7

二、去中心化的四种方式

具体来讲，去中心化主要包括四种方式：第一种方式是超额抵押，下面再讲到 MakerDAO 的时候，我会讲一下它的机制；第二种是跨链，比如说比特币如何在以太坊上面变成一个 ERC20 的 token，主要是在比特币的网络方面建立一种类似于 volt 储藏柜的机制，来实现它的一对一映射；第三种是弹性算法稳定币，在这种方式下，当币值与美元的汇率发生改变时，它要有一定的机制（增发或销毁）来稳定它的币值，但是在这个过程当中，其实还需要有外部的数据输入；第四种是部分储备稳定币，目前规模比较小。

如图 8，对于弹性算法稳定机制，它有一定的学术背景。在 2014 年有两篇学术论文提到，当时认为比特币不适合作为一种支付型的货币，那么什么样的支付型货币可以作为一种区块链原生态货币？这里

需要有一个稳定机制，有三种类型的弹性算法稳定币后来就被开发出来。一种类型是 AMPL，它需要把它和美元的汇率保持在 0.96~1.06 之间，然后这个概念需要有一种叫做 rebase 的方法，也就是调整它的基数，而调整它的基数主要是对于所有现存的 AMPL，它会同时采取或者是扩张或者是缩小这样的一个算法，来实现它和美元的汇率控制在一定的范围之中。另外一种方式，像 Basis，它其实不是说对于所有发出去的 token 进行一定的或者是通胀或者是通缩来让它和法币保持一定的稳定，而是说它会分成类似于股份和类似于债券，那么不同的稳定币通过这两种不同的这种机制，对于它另外一种所谓 BAC 的算法稳定币进行补充，或者是从它的整个系统中抽取，然后用这种方式来和法币进行一定的锚定。此外还有 ESD，它是类似于 Basis 这个方式，但是当中它少了一种支撑型货币。

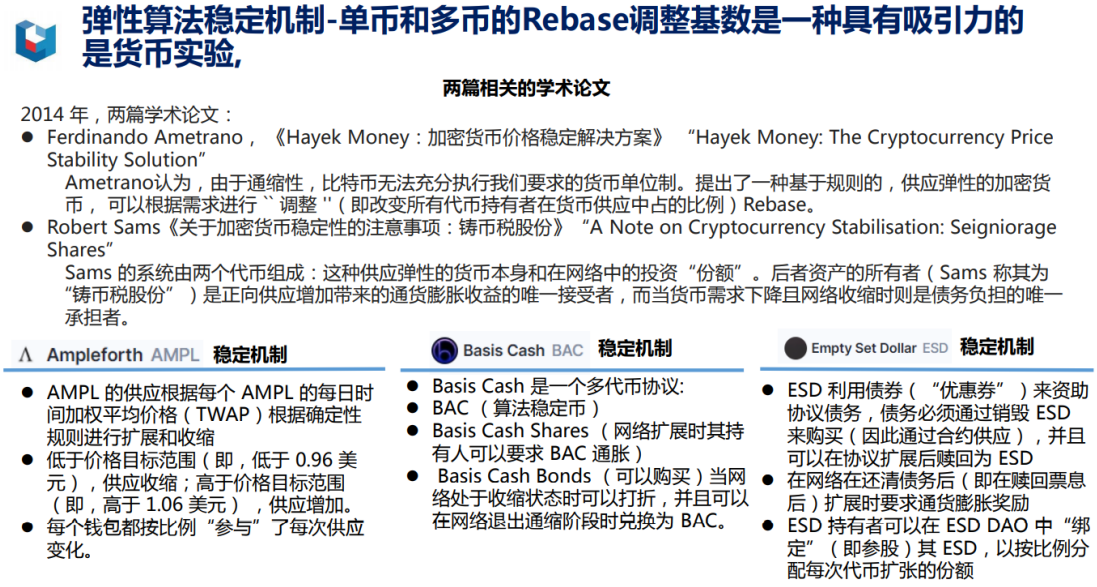


图 8

如图 9，在稳定币基础之上一个很重要的问题就是借贷。比如前

面提到了 AAVE，AAVE 是所谓的第二代数字银行或者是第二代的可以对 token 的存和取的一个 port 口，目前它的治理币是 AAVE，它的市值已经达到了 53 亿美元这么样的一个规模。

超额抵押是Defi借贷的主要方式，借贷是产生Yield Farming收益农耕的主要需求

	借贷	借贷机制	流通量	市值	价格
1	Aave AAVE	超额抵押、闪电借贷	12,487,074	5,358,820,481	429.15
2	Maker MKR	超额抵押	995,239	2,874,745,915	2888.50
3	Compound COMP	超额抵押	5,075,284	2,562,063,542	504.81
4	Venus XVS	超额抵押	9,424,362	783,820,744	83.17
5	Kava.io KAVA	超额抵押，多币种跨链	58,524,186	378,258,519	6.46
6	RAMP RAMP	超额抵押，多币种跨链	286,735,212	230,279,807	0.80
7	bZx Protocol BZRX	闪电贷款	192,714,950	160,006,283	0.83
8	HARD Protocol HARD	跨链货币市场	54,375,000	119,496,856	2.20
9	Cream Finance CREAM	基于Compound的P2P借贷	616,378	93,967,111	152.45
10	EasyFi EASY	基于Matic Network 的数字资产借贷协议	2,524,490	73,503,577	29.12
Total				12,474,956,552	

图 9

如图 10，MakerDAO 应该说是开启了整个 Defi 的 movement。在 2017 年的时候，它是第一次在不需要中心化、不需要人和机构介入的情况下，通过智能合约在以太坊上获得与美元汇率为 1:1 的稳定币，也就是通过 DAI 来实现这么一个功能。

MakerDAO 提供了以ETH超额抵押发放稳定币DAI,并用生态币MKR作为利息和治理币

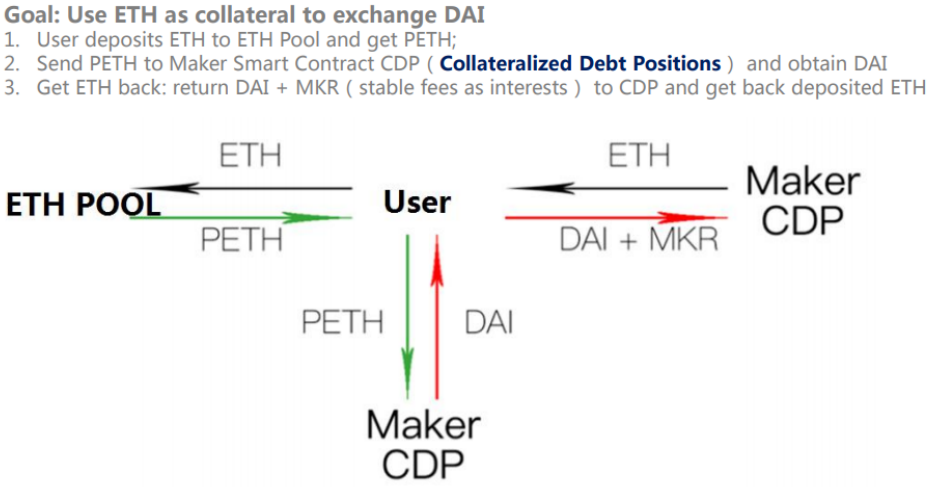


图 10

图 10 看起来较为复杂，主要原因是它背后的商业逻辑是当有人持有以太坊（PETH），那么当他把以太坊抵押给 MakerDAO 的智能合约，产生 maker cdp，这个叫做 collateralized debt positions。然后他又可以获得 DAI，之后用 DAI（DAI 和美元的汇率是 1:1）在以太坊上面用于投资，就是去买其他的一些币，当获得收益了以后，可以再还回来。问题是当他还回来的时候，利息的偿付是需要通过 MKR，MKR 实际上是 MakerDAO 的一个治理币，要获得 MKR，需要通过在市场上去购买，这是整个逻辑。

那么既然是通过抵押 ETH 来获得 DAI，这里有一个 over collateralization，即超量抵押的问题。超量抵押当时在抵押的时候是按照 150%，也就是说 MakerDAO 还是需要有外部的关于 ETH 价格的输入，所以它在 MakerDAO 里面其实有一个 oracle 的方式，也就是它有一个预言机来获得 ETH 的价格。不过，150%的 over

collateralization 也可能会产生问题，在 2020 年 3 月 12 日就出现了 ETH 暴跌了 50%以上（如图 11）。在这种情况下，MakerDAO 在整个清算和拍卖的过程中，出现了抵押在合约当中的 ETH 价格，实际上比它发行出去的 DAI 的价格要低。那么在这个时候，它其实已经产生了亏空，在当天的话这个亏空是 530 万美元。当然 530 万美元后来是 MakerDAO 的项目方从他们的基金会里面弥补了这一部分的损失。那么换一句话说，在这种去中心化的稳定币或者是去中心化的借贷当中，其实我们可以看到，还是有可能会出现违约的可能的。

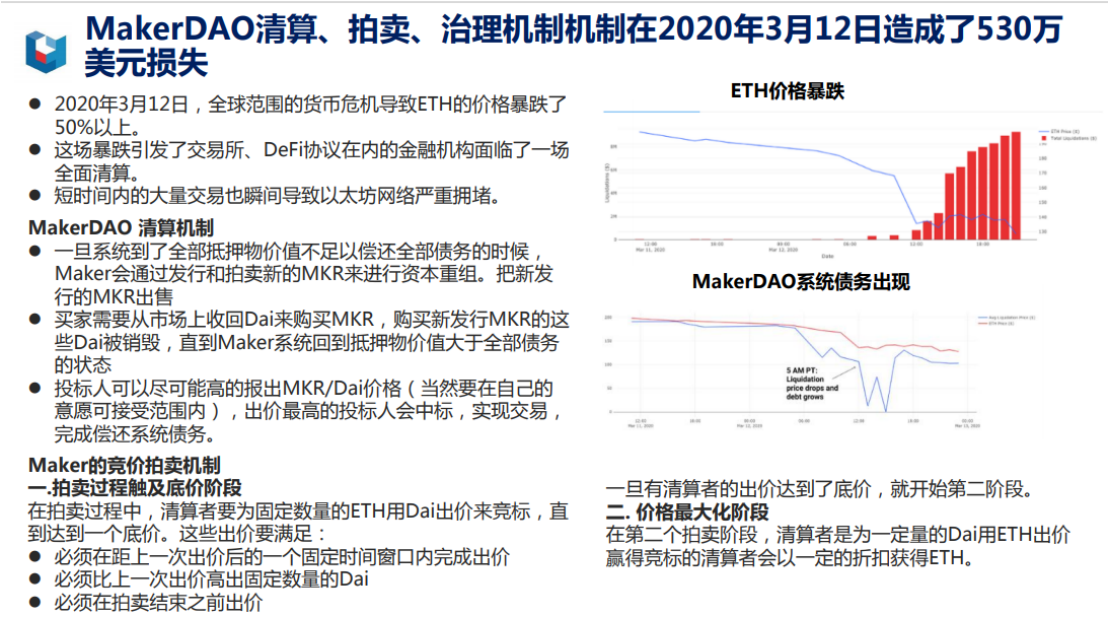


图 11

如图 12，在 MakerDAO 创造了算法稳定币之后， Compound 出现，这是第一代去中心化数字银行。当然它的设计概念一开始还不是按照银行的概念来设计，还是所谓的 money market fund。所以它里面有三个合约，一个是 money market 合约，一个是利率模型合约，另外有一个价格预言机的合约。它通过这三个智能合约构成了一个生

态，在生态里面，基于以太坊的 ERC20，基本上可以存，也可以借 ERC20 的 token，不同的 token 会有不同的利率。因为时间关系，我不详细讲 Compound 流程，但是它和 MakerDAO 一样，是第一代真正的实现了不需要中心化的银行机构。基于借贷和抵押的这样一种机制，通过三个智能合约，构建了当时模拟银行的存和取这样一个存取和借贷功能。

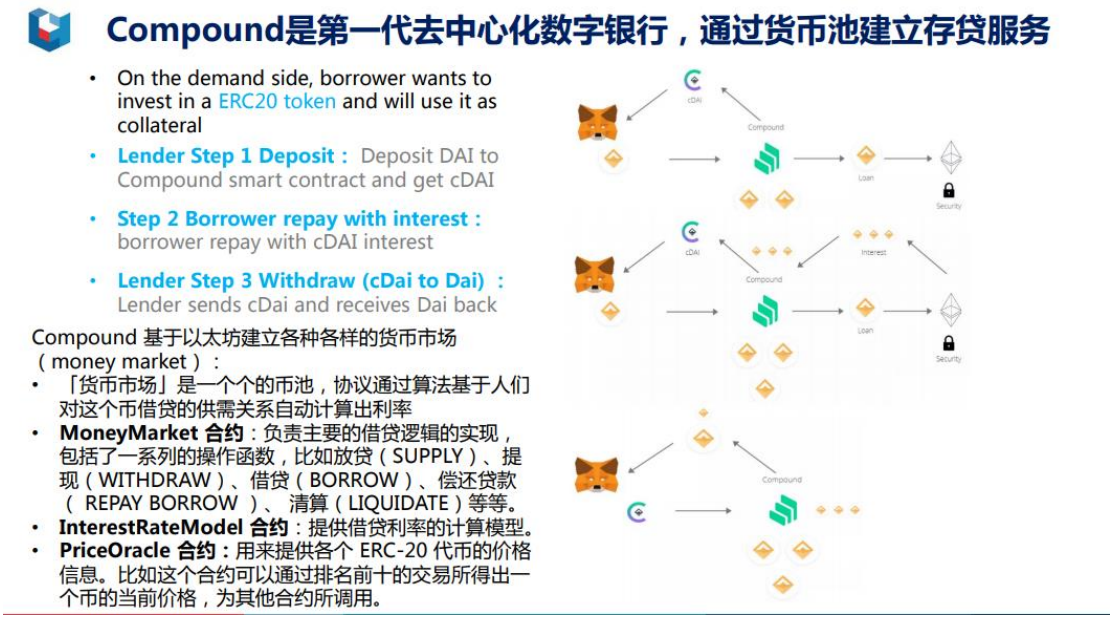


图 12

我们说 AAVE 是第二代去中心化数字银行，它实际上实现了一种功能叫做 Flash Loan，即闪电借贷。闪电借贷在我们讲的传统金融服务当中应该是不存在的。它之所以不存在，是因为它的概念是以一定的利息，非抵押大额的借贷。如果有人愿意借给你的话，你可以来做这件事情，但是有一个前提条件，它是在一个区块时间内完成了从借贷到还的过程，也就是说这一定是通过智能合约来实现的。比如说是通过 AAVE，可以来借比如说是 1 万美元的 Loan，当然这个 Loan

一定借的是 token。当然你如果能够借出来 ETH 的话，也可以立刻通过其他的 AMM 的机制，通过其他的去中心化的交易所可以换成稳定币。那么它的目的是什么呢？目的是如果有人能够发现在不同的交易所中有套利机会，那么它就有可能通过这种 Flash Loan 机制，调用大量的资金使这种套利的机会趋近于 0。

在图 13 上，我展示了一个案例，具体的流程非常清楚。但是我想讲的是这种 Flash Loan，第一在现实的金融功能当中没有这样的功能，第二是这个也非常危险。因为出现了好几次通过 Flash Loan 抓到了智能合约的漏洞进行套取，它不是一个对于交易所的一种套利。通过 Flash Loan 的这么一个过程，造成的损失可能有几千万到上亿美元，并且这样的损失已经发生了好几起。

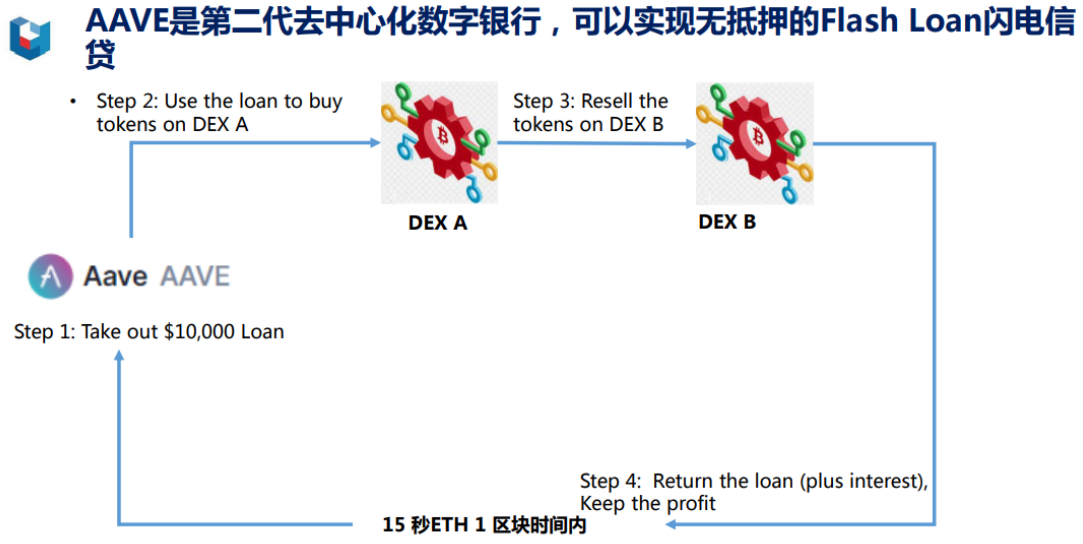


图 13

接下来，如图 14，我们来讲一下去中心化交易所。中心化交易所不管是 Lisi Nasdaq 还是其他的，我们知道都需要有 market maker，

有做市商，因为它是一个非常重要的问题，当有人想卖某种资产的时候，可能是没有足够多的人想买，那么你需要有流动性，有市场的深度。但是 Whiteley 最早提出来通过 AMM 这种自动做市的机制，可以在没有做市商的情况下，在你想买和卖的时候，通过流动性的池子（liquidity poor）来和你做交易对手。而且这种 liquidity pool 通过一定的数学公式，实际上可以寻找到合适的价格，而且这个价格如果一旦偏离了市场价格，这时候就产生了套利机会。所以 AMM 根本的金融原理还是希望市场上有大量的套利者，基本上可以使在不同的交易所，不管是中心化的还是去中心化的，都可以达到一个比较一致的市场价格。

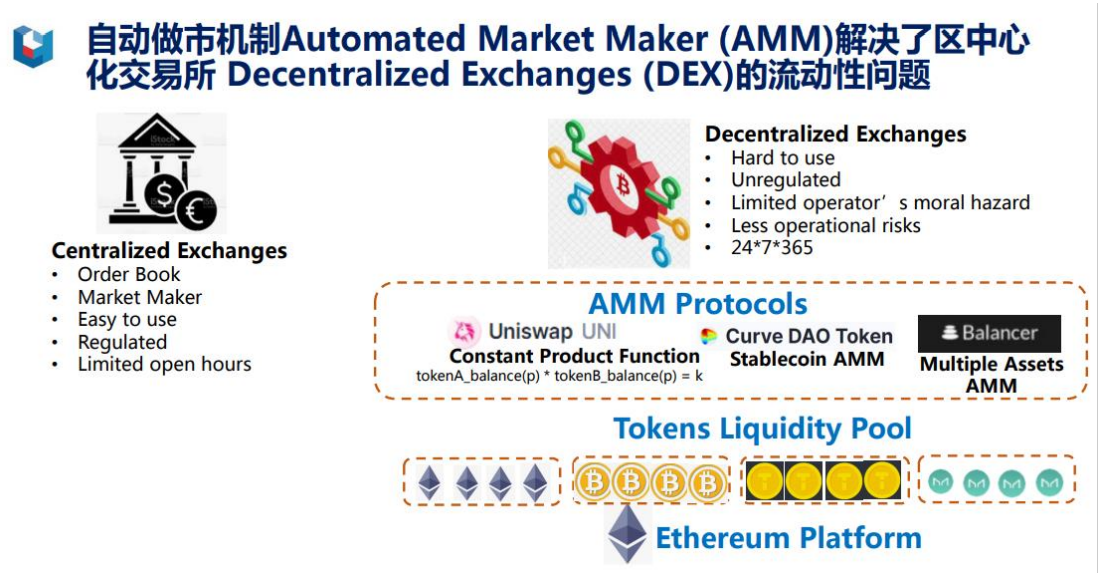


图 14

AMM 这种自动做市商的模式，从数学角度来看，有三种比较常见的形式，如图 15。而真正用得比较多的是所谓的恒定乘积，就是 x 乘以 y 等于 k。举一个例子，比如说比特币可能是 64000 美元，以太

坊假如说算是 2000 美元，那么比特币和以太坊的比值差不多应该是 1:32、1:31 左右的一个比例。那么当你做成了一个比特币和以太坊的一个对子后，也就是说有两个流动性池子。如果这两个池子足够大，比如说是一个池子里有 1 万个比特币或者甚至有 5 万个比特币，另外一个池子里有 5 万个比特币，它可能对应的是 150 万个以太坊。那么，在这种情况下，当你交易 1 个、2 个或者是 10 个比特币或者以太坊的时候，价格和它现在的市场价格差的是不会太多。但是这里也有一个很大的危险，就是说如果你两边的池子，即比特币和以太坊的池子都不够深、不够多的话，那么有可能当一个巨大的价格变化，或者是有人在交易所里进行了大笔的交易，有可能造成交易价格的和市场价格的一个巨大的偏离，实际上就是所谓的无偿的亏损 IL，impermanent loss。这就是我们讲的 AMM 这种自动做市商机制里面的一个最大风险。

除了 x 乘以 y 等于一个常数之外，还有其他的两个模式，虽然用的不太多。一个是 x 加 y 等于一个常数，还有一个是多种资产的乘积，或者是 square 或者是 1/3 次方是一个常数。这种常数都是可以保持当你两个池子足够深、足够大的情况下，它的价格是比较稳定的，比较符合市场价格的。

现在也有一些自动做市商 AMM 的增强模型，比如说 Curve，实际上是为了稳定币做的一个协议，所以它特别要求价格稳定，所以它有把恒定乘积以及恒定总和结合起来的一种新的方式。

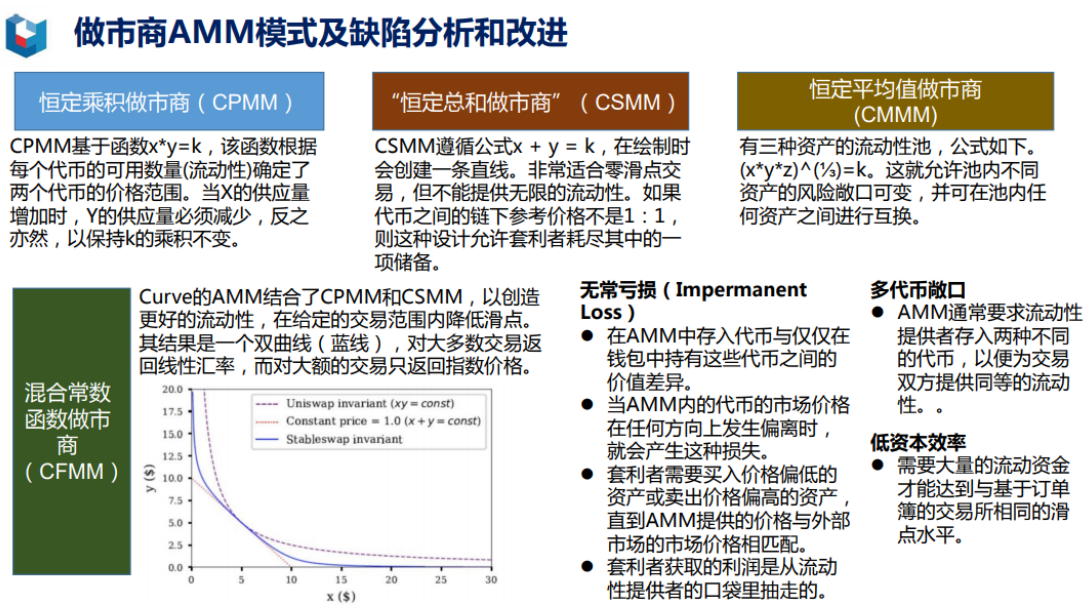


图 15

Uniswap 是最早实现以及交易对子最多的一个去中心化交易所，现在应该有 500 个对子到 600 个对子在 Uniswap。那么 Uniswap 之后，比如说 SushiSwap 以及后来币安做出来的 PancakeSwap 等等，都是类似的这种想法和做法。在这种基础之上，应该说是满足了很多交易的需求，在这种去中心化的交易所当中，甚至有很多流动性很差的这种小的币种，也可以进行交易。就像我刚才提到的，对于 AMM 交易机制来说的话，提供的流动性的池子越深越厚，它的安全性越好，它的价格发现机制也就越好。所以这种去中心化交易所的 AMM，如图 16，它是产生 liquidity mining（流动性挖矿，也就是有人可以把自己的 token 拿出来，放到流动性的池子里去，然后获得一定的利率的回报）的主要需求。其中，很多时候利率的回报可能是我们讲的治理币，即 governance token 这么一种回报，而不是说抵押了 ETH，然后获得 ETH 本身的利率的回报。

DEX的AMM是产生Liquidity Mining流动性挖矿的主要需求

	DEX	AMM 机制	流通量	市值	价格
1	Uniswap UNI	链上token pairs自动交易	523,384,244	19,888,203,273	38.0
2	PancakeSwap CAKE	基于币安智能链的DEX	152,675,144	3,591,746,529	23.5
3	SushiSwap SUSHI	UniSwap的分叉	127,244,443	2,278,982,416	17.9
4	Bancor BNT	通过智能合约为数字货币提供持续流动性	178,550,078	1,383,148,382	7.7
5	1inch 1INCH	集成了大量的DEX	156,671,623	930,127,951	5.9
6	Curve DAO Token CRV	稳定币DEX	273,116,186	898,736,380	3.3
7	Kyber Network KNC	DEX让商家处理任意的通证付款功能的支付API	205,045,092	723,021,273	3.5
8	ZKSwap ZKS	提供无限可扩展性和隐私性Uniswap的全套功能	197,440,000	625,543,941	3.2
9	Balancer BAL	DEX和资产管理平台	6,943,831	494,043,640	71.1
10	BakeryToken BAKE	质押、“烘焙”、创造独特的NFT	188,717,930	325,018,218	1.7
Total				31,138,572,003	

图 16

如图 17，我们可以看一下 UniSwap 以及 UniSwap 本身的通证经济学，也就是 governance token 的一个分配机制，那么它是一个 UNI，UNI 本身并不代表更多的经济利益，但是持有 UNI 的话，可以参与到整个社区的对于 UniSwap 的管理。同时，因为 UniSwap 是一种交易型的协议，所以它可以收 commission，然后 commission 主要是回馈给 LP（liquidity provider，流动性的提供方），0.3%的交易费用。

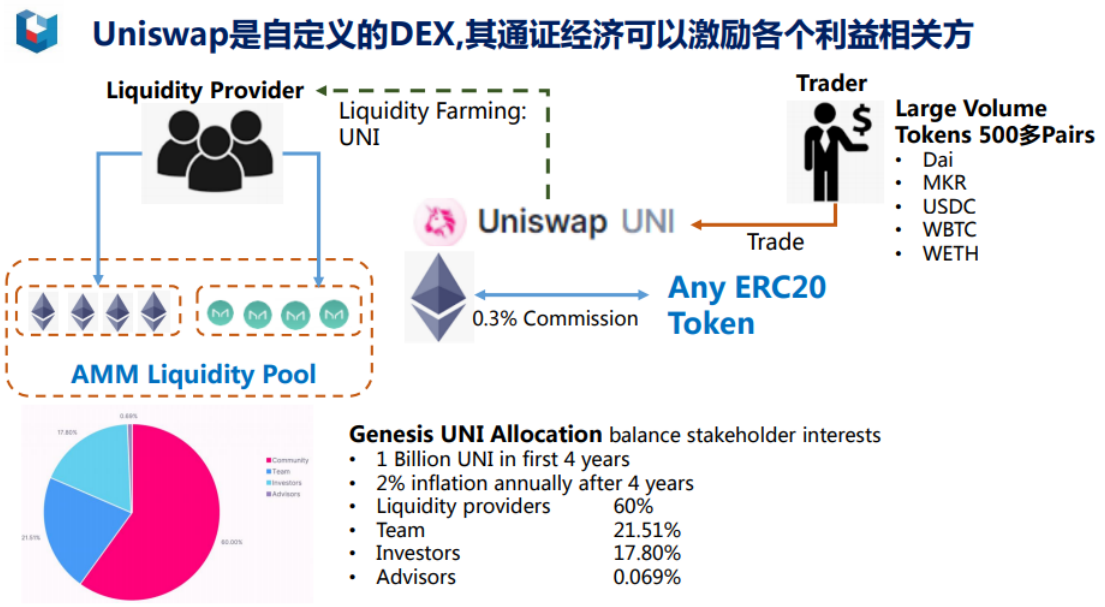


图 17

我们再看一下除了交易所之外，还有资产合成，如图 18。资产合成最早的第一代是 Synthetix，它通过一种类似于 MakerDAO 的机制可以把任何链上和链下资产进行合成。其中，涉及资产主要是链下实体经济或者是现实社会当中的这些资产，由于这些资产是权益类资产，所以它的抵押 over collateralization 就更高，达到 700%的 over collateralization。然后，它在链上主要是发行与资产对应的 token，然后针对 token 进行运作。Synthetix 和 UMA 都是这种资产的合成方式。

链上和链下资产的合成将具备巨大的发展潜力

	资产合成	资产合成机制	流通量	市值	价格
1	Synthetix SNX	任何链下资产的链上合成资产平台	114,841,533	2,371,159,047	20.6
2	UMA UMA	任何链下资产的链上合成资产平台	60,074,001	1,600,774,257	26.6
3	Mirror Protocol MIR	美股超额抵押合成资产	55,076,299	516,328,630	9.4
4	Standard Tokenization Protocol STPT	资产在全球范围内合规框架下发行通证	1,025,143,223	87,939,582	0.1
5	Jarvis Network JRT	任何链下资产的链上合成资产平台	29,005,880	5,257,618	0.2
Total				4,581,459,134	

图 18

我们可以看一下 Synthetix 的运行机制，如图 19，它包括了美元、欧元等货币，包括了大宗商品经营，也包括了比特币、以太坊，还有比特币、以太坊的反向收益的一种合成型的资产 token。它需要经过铸造、交易和燃烧三个步骤来实现，主要讲的是这个 token，包括 token 的发行、交易以及最后的销毁。在这里它需要锁定 SNX，SNX 是 Synthetix 它本身自己发行出来的币，这个币实际上是需要购买，也就是在 Synthetix 要铸币的人需要买。现在对于这种合成资产，应该说是有巨大的潜力，这里包括了有中心化和去中心化的做法。我们看到币安对于 Tesla，对于 Coinbase，它实际上都是通过中心化的手法发出来 STO，Security token。当然这种 STO 和美国 SEC 所定义的 STO 是不一样的概念。

通过这种去中心化的手法来发行合成的证券，也包括有镜像的 protocol 以及其他的一些尝试。我个人认为去中心化的发行证券可能未来会有非常大的潜力，如果是从合规以及从技术和算法的角度有所突破的话。

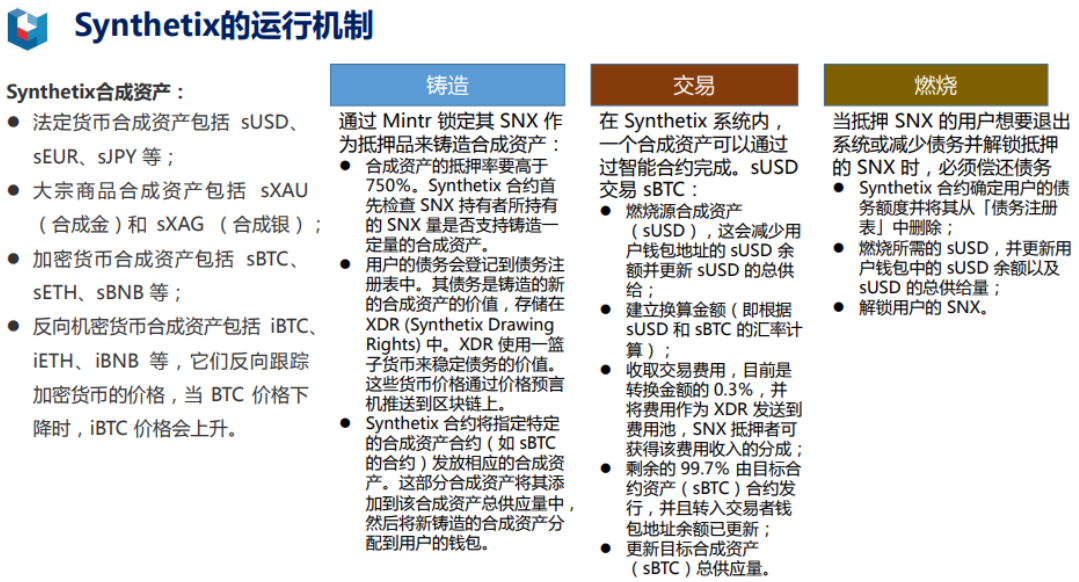


图 19

不仅是借贷和投资资产合成、资产管理，保险在去中心化金融 Defi 里也开始发展起来了，尤其是 Nexus Mutual，如图 20，也有很多这种创新的点子。前面我们讲到通过 Flash Loan 已经出现了多次的损失，主要是黑客对智能合约的攻击，那么，有没有什么办法来进行保护？

Nexus 开发出来了比如说是智能合约的保险，比如说是资产托管的保险，而且它确实实现了赔付，它已经有 14 次赔付，赔出去差不多 250 万美元的 ETH 和 DAI 稳定币。那么，Nexus Mutual 在其背后的设计当中，应该说是非常符合保险的原理，它有一个 shield pooling，也就是保护伞或者是保护盾。当你向 shield pool 里贡献了 token 的话，那么你实际上可以获得保险的回报。也就是说，如果没有出险的话，可以来分保费，当然这些保费也是以 token 的形式来进行支付；当然如果出险了，你自己投出去的 token 可能就会损失掉。现在在差不多

接近 1000 个亿的 locked value（锁住价值）当中，大概仅仅只有 1%~2% 左右是为了这个保险。

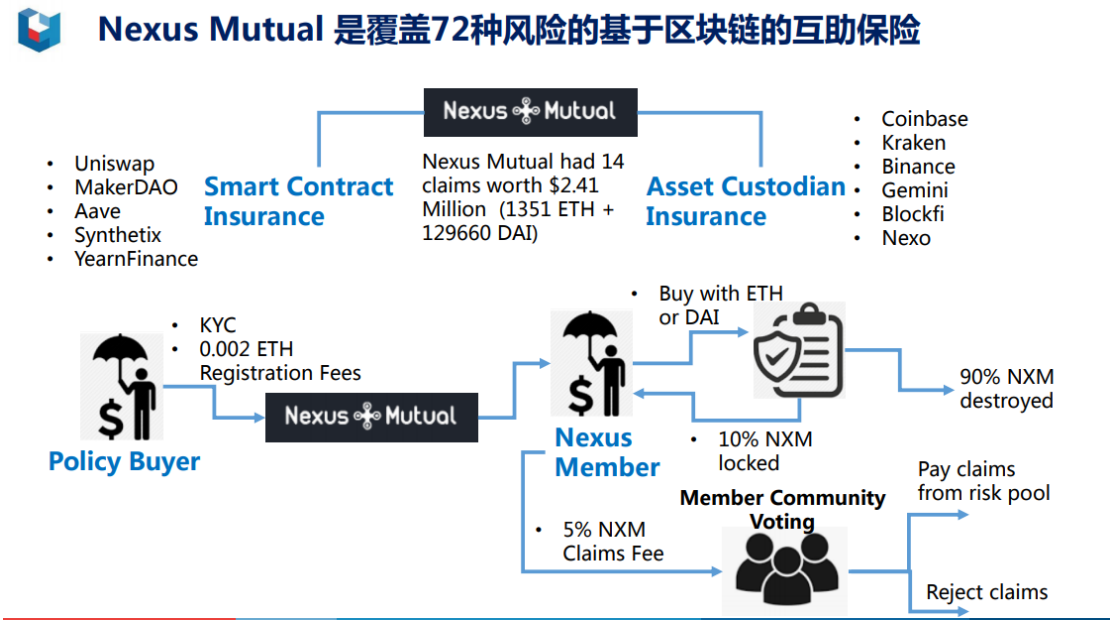


图 20

如图 21，显示的是到今天为止，整个的这种 TVL，整体的锁仓量达到了接近 1000 亿美元。

图 21

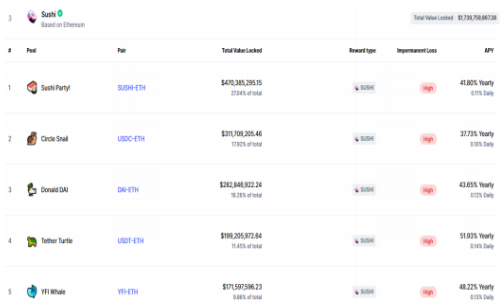
我希望通过前面这个介绍大家可以理解，由于去中心化金融里的自动做市，或者是抵押借贷或者是资产合成等等的这些金融功能，它

其实都是需要有人来贡献这个 token。但是它并不是为了交易，不是为了卖掉 token，而是作为贡献来实现一些金融功能。比如说提供交易的流动性，比如说通过保险来提供保护，比如说是在稳定币当中提供 collateral 等。但是，在这种所谓的抵押，或者叫 staking，或者叫 farming 的这种活动当中，它其实实现了一个非常重要的对于币，即 token 的一个跨越，它的本质的跨越就在于持有币是可以获得利息的，是可以获得一定的回报。当然你在从事不同的抵押行为的时候，它的风险也不一样。

比如说我们可以看到图 22，在不同的生态当中的抵押，也可能会造成损失。所以我们看到在 Sushi，其实是 UniSwap 的一个分差，有一些创新的方法，主要是拉动生态、生态的冷启动等等这些运营方法。Sushi 因为可能涉及的是任意资产的交易，所以它的风险比较高，那么它对应的利率也比较高。而 Curve 实际上是为了实现稳定币，那么它相对来讲风险比较小，所以在 Curve 的生态当中，抵押的 token 可能获得的这种所谓的利息也会比较少。

Yield Farming在不同的系统里获得不同的“利息回报”

Sushi生态里的“利率”较高



Curve稳定币生态里的“利率”较低

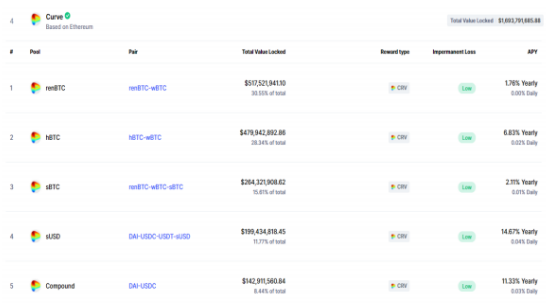


图 22

最后，现在比特币再加上其他所有的我们讲到的这些 Defi 的生态，它们的总价值已经达到了 2.2 万亿美元这样一个规模，已经变成了一个非常显著的资产类别。

那么更重要的是，我们可能需要去理解 Defi 对于金融真正产生了什么样的影响？有什么样的意义？第一点，我认为 Defi 的这些创新机制非常有价值，它必然会走向实体经济，服务实体经济。也就是说这些 Defi 的机制，它会和现有的金融机构的一些金融功能结合起来，诞生出新的金融服务的方式，最终可以服务实体经济的发展。

第二点是我个人的观点，就是可能未来非人的智能设备的兴起。也就是说，无人驾驶汽车、智能的 IOT 等等。这些智能的设备，它可能会需要类似于我们现在讲的金融服务，也就是说需要一定的资源支持，资源分配、聚合等，而这样的需求当它出现的时候，现在 Defi 的这些算法和机制设计会起到非常大的作用。

第三点就是最终监管需要和 Defi 的发展适配。如同前面提到的，虽然现在 Defi 从真正参与的人数来讲，是非常有限的。每一个 protocol 可能就只有几千人、几百人在做，最大的可能也就是上万人。但是未来它发展起来了以后，尤其是它现在的这种 Dollar Amount，它影响到的金钱数量已经有明显的增长，所以最终还是要有一定形式的监管适配与 Defi 的发展结合起来，而不是像现在这种几乎没有监管的发展状态。

三、问答环节

Q1：Defi 在保险领域的应用目前怎么样？您觉得哪些方面可能有大的应用突破？

A1：目前对于链上的 Defi，已经有了智能合约和资产托管保险，对于链下，Defi 还没有保险应用。我觉得链下资产上链，非标 NFT 等都已经开始有爆发的迹象了。

Q2：是否可以谈谈您对于脸书体系下的数字货币的远景的一些想法？

A2：我觉得脸书的 Diem 现在处在等监管的状态，随着 Gary Gensler 开始上任，可能美国有各种监管政策的变化会出来。

Q3：Defi 能否和央行主导的数字货币联系起来？

A3：Defi 肯定可以和 CDBC 结合地很好，之前这么多稳定币的努力，就是没有原生态的数字法币。所以借贷、投资、保险都可以很好地利用 CBDC。现在一些稳定币的协议可能要退出市场。

Q4：请简单介绍一下罗汉堂的新方向或产品进展？

A4：罗汉堂前不久发布了数据和隐私报告，现在在数字经济和数字金融的多个方向上都陆续有产出。欢迎关注我们的网站和公众号。

本文根据北京大学汇丰金融研究院执行院长巴曙松教授发起并主持的“全球市场与中国连线”第三百五十三期（2021 年 4 月 15 日）内容整理而成，特邀嘉宾为罗汉堂资深专家邱明。

邱明先生现任罗汉堂资深专家，前蚂蚁金服研究院副院长，负责全球金融科技创新、国际金融监管政策，以及区块链等新科技的应用研究。邱明先生有 14 年的精算、交易、证券化、风险管理和资产负债管理的金融从业经历。他曾先后供职于美国贝尔斯登和摩根大通两家投资银行，亦在两家知名机构的纽约和伦敦交易前台任保险资产证券化产品交易员。之后还担任美国国际集团 (AIG) 的副总裁（VP），参与公司风险管理、资产负债管理，以及全球资产分析、汇总、及报告。邱明先生在哥伦比亚大学取得金融方法硕士学位，拥有三一大学计算机科学及数学学士学位。并拥有多项专业认证，其中包括：FSA (北美精算师协会会员)、MAAA (美国精算师学院会员)、FRM (金融风险管理师)、CAIA (注册另类资产投资分析师)、PRM (专业风险经理)、CHP (认证对冲基金管理师) 和 ERP (能源风险分析师)。

【免责声明】

“全球市场与中国连线”为中国与全球市场间内部专业高端金融交流平台。本期报告由巴曙松教授和王志峰博士共同整理，未经嘉宾本人审阅，文中观点仅代表嘉宾个人观点，不代表任何机构的意见，也不构成投资建议。

PHBS HFRI

北京大学汇丰金融研究院