

## 区块链进化史—— DeFi开启去中心化金融时代

2021-6-1

证券分析师：熊莉 xiongli1@guosen.com.cn 证券投资咨询执业资格证书编码：S0980519030002



## 1、区块链技术 1.0：比特币—去中心化、抗通胀、加密的全球数字资产

- 1.1 比特币的诞生背景
- 1.2 比特币背后的技术原理
- 1.3 比特币挖矿耗能情况分析
- 1.4 比特币的投资价值
- 1.5 比特币的持仓分布
- 1.6 全球企业和金融机构配置对比特币价格的潜在影响

## 2、区块链技术 2.0：智能合约—基于编程语言运行在去中心化网络上的不可篡改的合同

- 2.1 智能合约的产生背景
- 2.2 智能合约的应用案例

## 3、区块链技术 3.0：DeFi—基于智能合约发展的去中心化金融生态

- 3.1 DeFi的发展历程和生态现状
- 3.2 DeFi应用—借贷（抵押数字资产贷出数字资产）
- 3.3 DeFi应用—去中心化交易所（Decentralized Exchange）
- 3.4 DeFi应用—去中心化衍生品（合成资产案例）
- 3.5 DeFi应用—去中心化保险
- 3.6 DeFi应用—机枪池、实现资产收益最大化

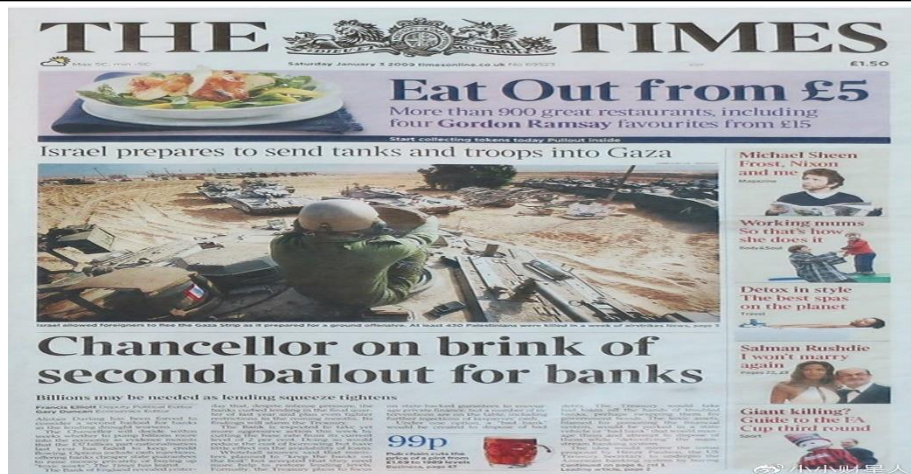
## 4、风险提示

## 区块链1.0：比特币——去中心化、抗通胀、加密的全球数字资产

# 比特币的诞生背景——对抗金融危机下的无限量宽松

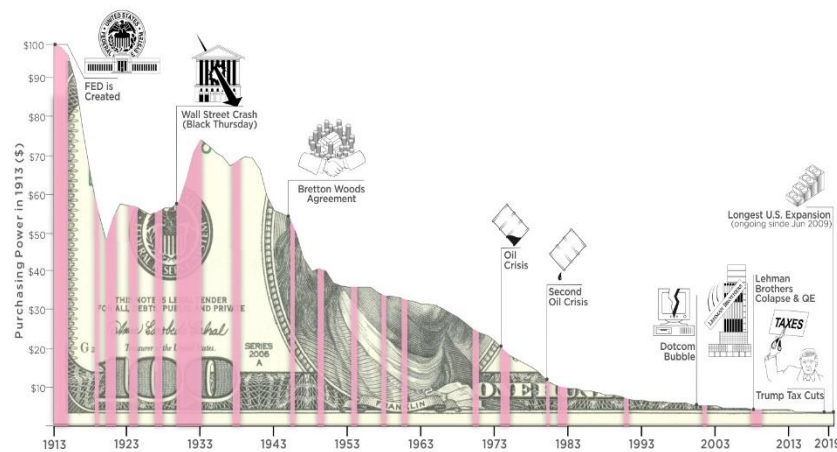
- **2008年11月**，比特币正式诞生，中本聪首次在网上发表了比特币的白皮书，其标题为《比特币：对等网络电子现金系统》(Bitcoin: A Peer-to-Peer Electronic Cash System) 整个论文详细论述了如何通过对等网络来创造一种“不需要依赖信任的电子交易系统”。
- **2009年1月3日**，比特币的区块链网络上出现了第一个区块，也被称为创世区块。在挖出首个区块后，中本聪在区块上留下了一句话，“The Times 3 January 2009 Chancellor on brink of second bailout for banks”，是当天泰晤士报的头版标题。08年发生金融危机后，全球央行开启了量化宽松，缓解市场的资金压力，这句话正好记录了在09年1月3号，财政大臣正处于实施第二轮银行紧急援助的边缘。
- **2010年12月12日**，这一天也是比特币历史上的重要一天，比特币创始人中本聪在Bitcointalk上发表了最后一篇稿子，从此销声匿迹。

图1：2009年1月3日泰晤士报标题



资料来源：国信证券经济研究所整理

图2：影响美元购买力的核心事件

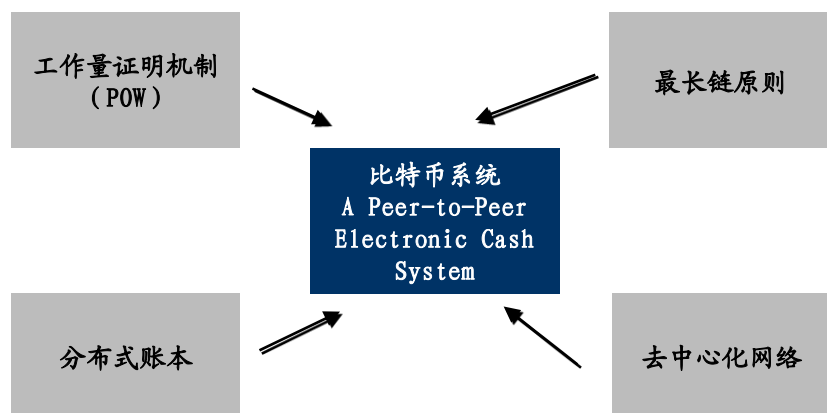


资料来源：国信证券经济研究所整理

# 比特币背后的技术原理——区块链技术

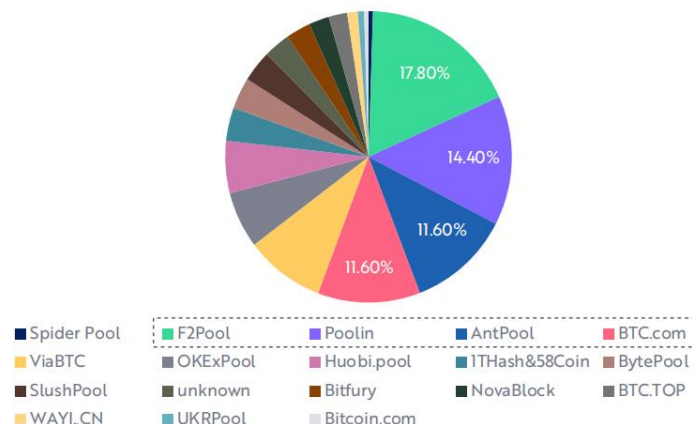
- 比特币的底层重要技术是区块链（Blockchain）技术，区块链技术也起源于比特币，**本质上是一个去中心化的数据库**。简单理解，区块链将原来中心化传统机构的“账本”，分布在全球所有的参与节点上，每个节点都充当记账的角色。比特币网络会动态调整打包区块的速度，平均每10分钟一个新的交易区块会被添加到总账本中，人们称之为“区块链”。区块链包含了自比特币系统启动以来所有的历史交易记录。**截止2021年6月1日，目前总共有将近68万个区块完成打包，总共大小约348GB左右。**
- **工作量证明机制（PoW）**：比特币网络中的节点按照规则进行加密哈希计算，以竞争获得生成新区块的权利。**每个区块的产生都需要解决一个数学难题，这个数学难题只能通过暴力计算和多次试错来解决。**节点在竞争获胜后就获得记账权，它生成区块成为最新区块后，就获得与新区块对应的挖矿奖励。**工作量证明也是区块链账本的安全机制。**如果不重做“工作量证明”所需的大量计算则此链条不可修改，这一共识机制保证了区块链上的数据的可靠性。
- **最长链原则**：在任何时刻，最长的链条是所有人都接受的最终记录。

图3：比特币系统设计的五大要点



资料来源：国信证券经济研究所整理

图4：比特币网络全球算力的分布

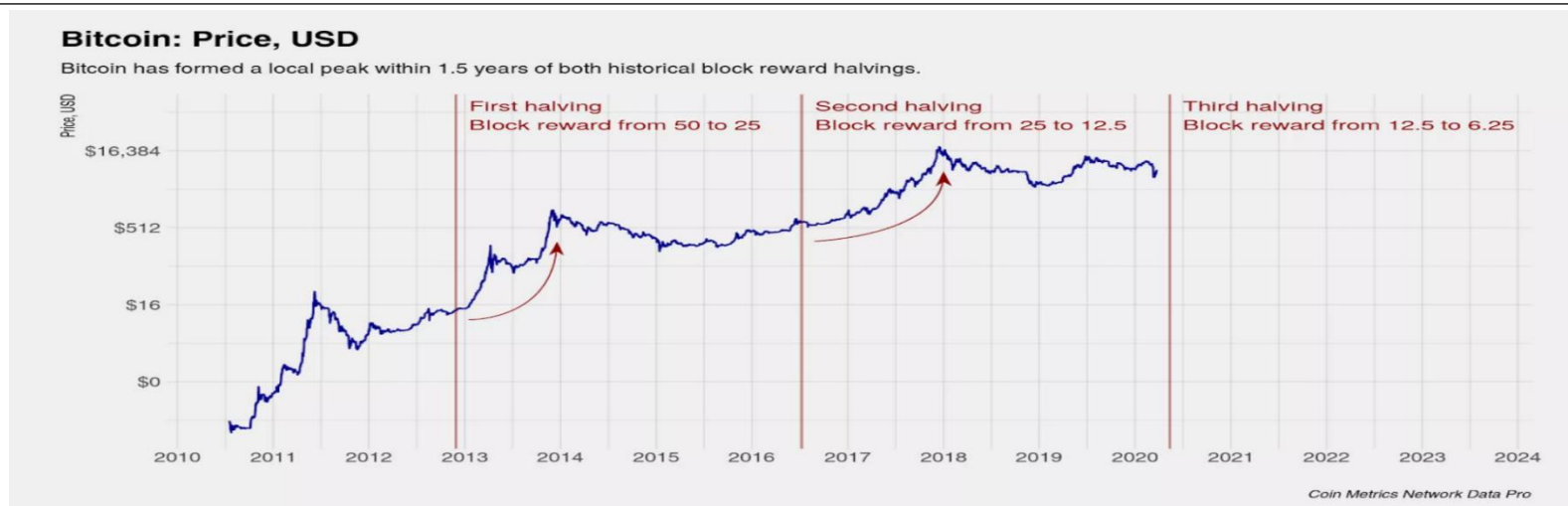


资料来源：ARK官网、国信证券经济研究所整理

# 比特币背后的技术原理—减半周期设定

- 根据比特币的原始代码的设定，基于工作量证明机制（POW）的挖矿，每隔21万个区块，矿工的奖金就会减半(大约每隔四年发生一次)。比特币最早的供应是每个区块50个比特币，21万个区块挖出后该奖励降低到25个比特币，然后到2016年每个区块奖励变得只有12.5个。最近一次减半发生在2020年5月，每个区块的奖励已经降至6.25个。
- 供应减半是很难被预先定价的。减半预期会影响供求关系，从而影响价格，进而影响事件中的潜在价格。但是实际减半发生后，看起来被“定价”了的比特币，在需求稳定的情况下，价格仍会上涨。但是在历史上由于每轮减半的数量随着时间推移而减少，相应对供给格局的影响也在减弱。整个挖矿奖励减半的机制将延续到2140年左右，在那之后，矿工确认交易的奖励将会转为由网络上的用户所支付。比特币网络上的竞争将会促使交易费用维持在较低的水平。

图5：比特币历年减半价格走势



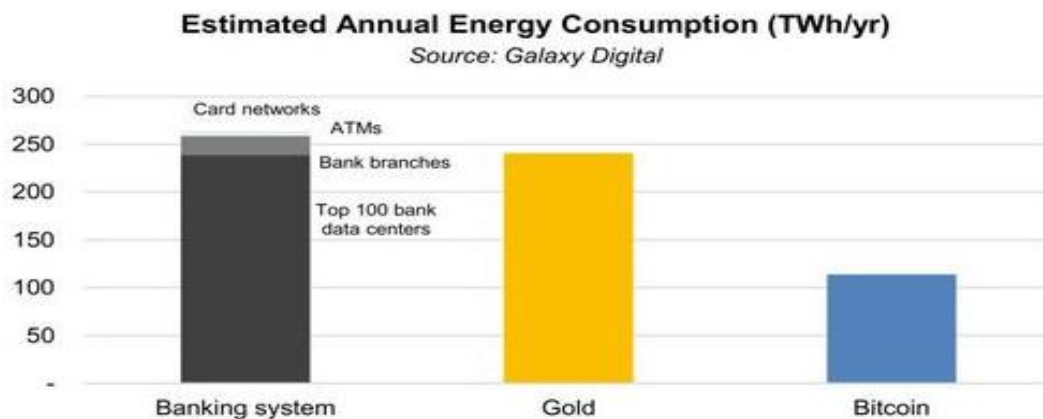
资料来源：Wind、国信证券经济研究所整理



# 比特币挖矿耗能情况分析

- **比特币、黄金、全球银行体系耗能对比：**剑桥大学比特币耗电量指数的数据显示，比特币挖矿每年耗电量预计为115太瓦时（1太瓦时为10亿度电），约等于全球发电量的0.51%。假设每年黄金产量约2500-3000吨，将消耗约132太瓦时的电力。Galaxy Digital数据指出，相比起比特币的能耗使用，传统金融行业的耗能相对较复杂，假设我们考虑运行全球所有ATMs、银行营业部、支付系统以及银行数据中心，光电力的消耗将超过260太瓦时。
- 考虑到挖矿支出是维系比特币体系运行的最主要成本，在与传统银行体系对比的同时，我们还需考虑维护传统银行体系电力以外的成本，比如银行体系的管理成本、印钞成本、假币干扰及反假币行动成本等。**剑桥大学数字资产研究报告指出，全球39%的基于工作量证明挖矿机制下的电力消耗来自于可再生能源。**比特币矿业可能会对可再生能源的发展产生积极影响，比如通过储能的方式将间歇性电力资源转化为基本负载发电，从而影响向电网供应的可再生能源的数量。

图6：比特币耗能对比



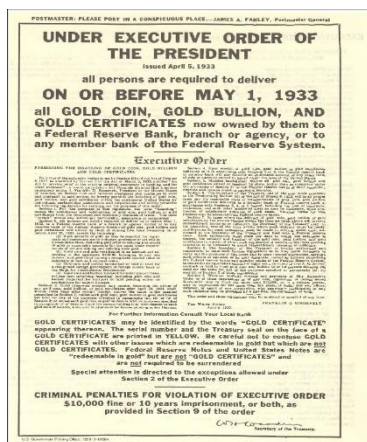
资料来源：Galaxy Digital、国信证券经济研究所整理

# 比特币投资价值——继承黄金重要属性，数字化使其更优

➤ 比特币不仅继承了黄金的全部重要属性，同时还具有黄金无法比拟的优势：

- **抗通胀，用于价值存储：**总量恒定2100万个，目前已经挖出1869万个左右。比特币的最小单位为一聪，相比黄金更易于分割。
- **数字化，易于转移和携带：**比特币可以在全球网络内，以绝对安全的方式进行转移，只需要付出数美元的手续费和十几分钟耗时便可完成转账，不依赖任何第三方结算。比特币在全球数千个数字资产交易所24小时365天交易。
- **去中心化，不依赖机构背书：**比特币的每一笔交易，都由区块链上的所有节点确认，而不依赖于某一中心化机构背书，因此大幅提升了抗攻击性。在去中心化的部署下，黑客无法通过攻击某一节点而使整个网络瘫痪，对去中心化系统进行攻击破坏的成本相比中心化系统更高。同时比特币网络上的每一个节点都是平行的，不存在上下级和主从的关系。

图7：1933年美国政府宣布没收私人黄金的海报



资料来源：国信证券经济研究所整理

图8：金本位下的美元



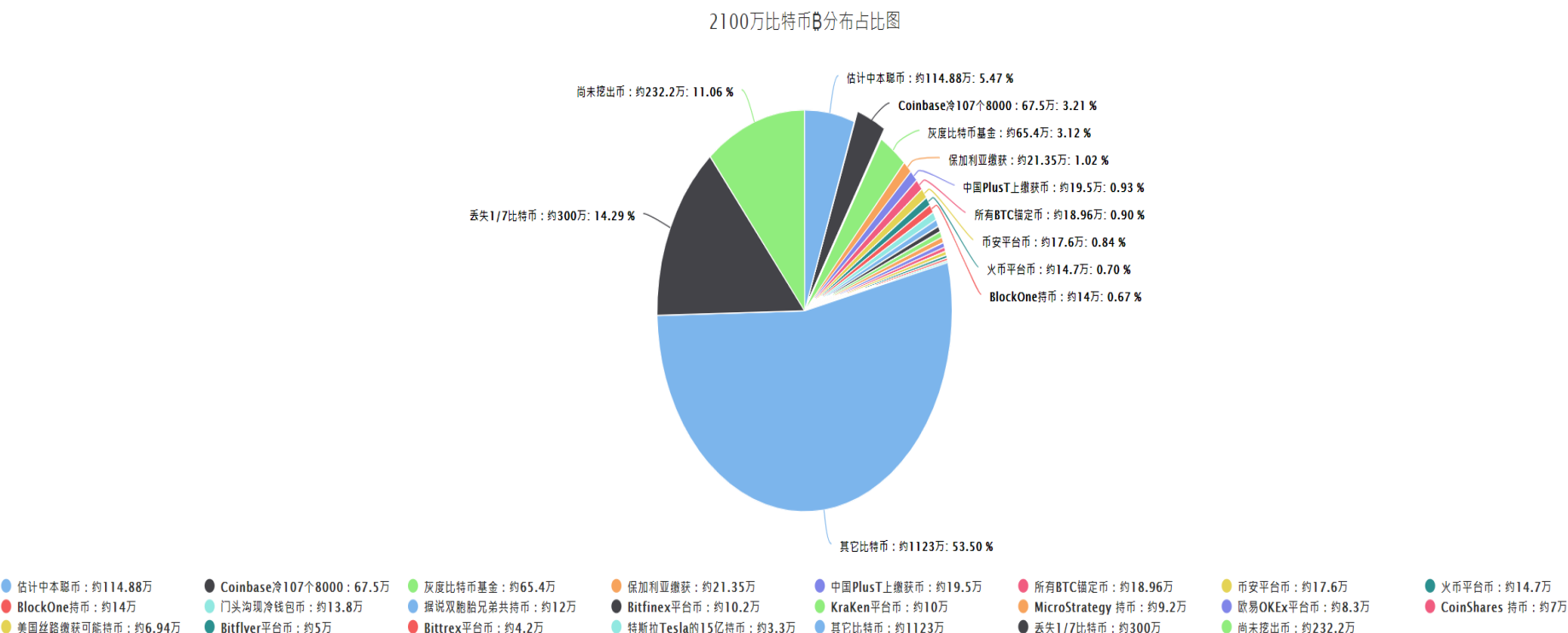
资料来源：国信证券经济研究所整理



# 比特币持仓分布——头部持币地址多数为数字货币交易所

- 比特币在全球的持仓分布较为分散，头部持币地址大部分来自于数字货币交易所。根据2013年Sergio的一篇文章分析指出，中本聪的持币数量为114.88万个。有证据显示比特币网络前36000个区块都是由同一台电脑挖出的，挖矿的人很可能是中本聪。

图9：比特币持仓分布（更新于2021年5月7日）



资料来源：ofbtc.com、国信证券经济研究所整理

# 比特币持仓分布—全球上市公司持仓

➤ 根据上市公司公告统计，全球目前有23家上市公司持有比特币，总共持有180,335枚比特币，约占比特币总量的0.96%。

图10: 全球上市公司持有比特币的数量统计

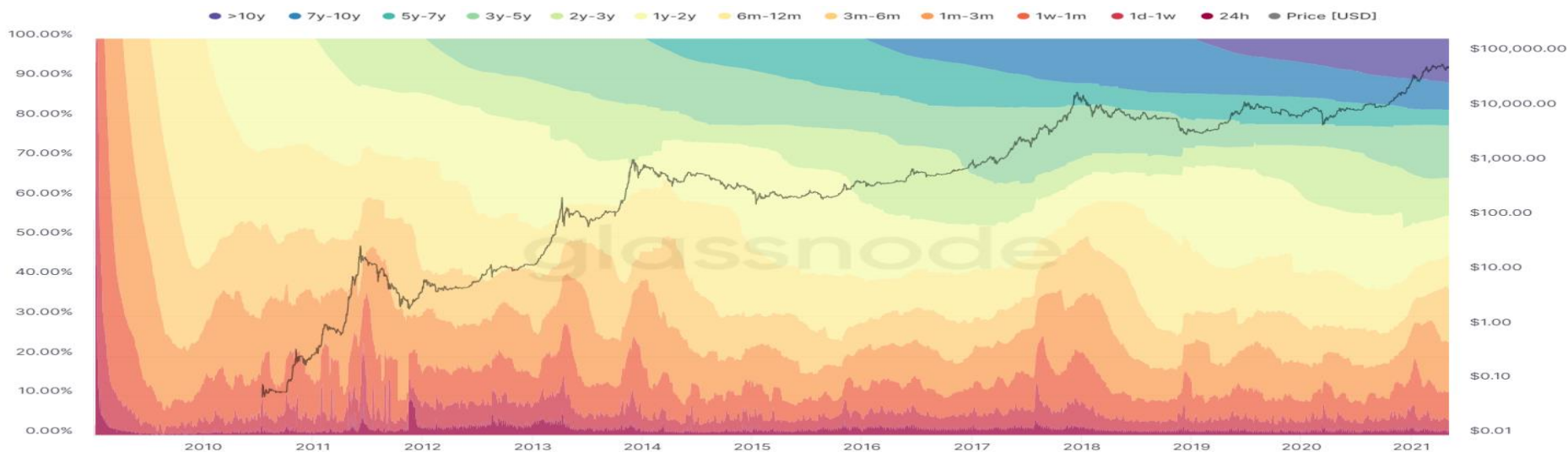
#	Company 上市公司	Symbol 股票代码	Country 上市国家	Total Bitcoin 持有比特币数量	Entry Value (USD) 购买时的持仓市值	Today's Value (USD) 2021年5月7日持仓市值	% of Total BTC Supply 比特币总量占比
1	MicroStrategy Inc.	NASDAQ:MSTR	US	91,579	<a href="#">\$2,226,000,000</a>	\$5,134,322,905	0.44%
2	Tesla	NASDAQ: TSLA	US	48,000	<a href="#">\$1,500,000,000</a>	\$2,691,091,838	0.23%
3	Galaxy Digital Holdings	TSE:GLXY	CA	16,402	<a href="#">\$134,000,000</a>	\$919,568,507	0.08%
4	Square Inc.	NASDAQ:SQ	US	8,027	<a href="#">\$220,000,000</a>	\$450,029,046	0.04%
5	Marathon Patent Group	NASDAQ:MARA	US	4,813	<a href="#">\$150,000,000</a>	\$269,838,021	0.02%
6	Hut 8 Mining Corp	TSX:Hut-8	CA	2,851	<a href="#">\$36,788,573</a>	\$159,839,642	0.01%
7	NEXON Co Ltd	TYO: 3659	Japan	1,717	<a href="#">\$100,000,000</a>	\$96,262,598	0.01%
8	Voyager Digital LTD	CSE:VYGR	CA	1,239	<a href="#">\$7,927,182</a>	\$69,463,808	0.01%
9	Riot Blockchain, Inc.	NASDAQ:RIOT	US	1,175	<a href="#">\$7,200,000</a>	\$65,875,686	0.01%
10	Aker ASA (Seetee AS)	OL:AKER	NO	1,170	<a href="#">\$58,599,450</a>	\$65,595,364	0.01%
11	Meitu	HKG:1357	HK	940	<a href="#">\$49,500,000</a>	\$52,749,325	0.00%
12	Coin Citadel Inc	OTCMKTS:CCTL	US	513	<a href="#">\$184,390</a>	\$28,761,044	0.00%
13	Cypherpunk Holdings Inc	CSE: HODL	Canada	350	<a href="#">\$5,637,663</a>	\$19,622,545	0.00%
14	Advanced Bitcoin Technologies AG	ABT:GR	DE	254	<a href="#">\$2,117,978</a>	\$14,240,361	0.00%
15	BIGG Digital Assets Inc.	CNSX:BIGG	CA	239	<a href="#">\$2,690,387</a>	\$13,399,395	0.00%
16	Cypherpunk Holdings Inc.	CSE:HODL	CA	235	<a href="#">\$1,630,000</a>	\$13,175,137	0.00%
17	DigitalX	ASX:DCC	AU	215	<a href="#">\$874,835</a>	\$12,053,849	0.00%
18	Hive Blockchain	CVE:HIVE	CA	211	-	\$11,829,591	0.00%
19	Fortress Blockchain	TSXV:FORT	CA	163	-	\$9,149,712	0.00%
20	Mode Global Holdings	LON:MODE	UK	85	<a href="#">\$975,089</a>	\$4,765,475	0.00%
21	Neptune Digital Assets Corp.	TSXV: DASH	CA	75	-	\$4,204,831	0.00%
22	FRMO Corp.	OTCMKTS:FRMO	US	63	-	\$3,532,058	0.00%
23	Mogo Inc.	NASDAQ:MOGO	CA	18	<a href="#">\$595,494</a>	\$1,009,159	0.00%

资料来源: coingecko.com、国信证券经济研究所整理

# 比特币衍生的金融资产

- **比特币信托**: 2013年9月, 灰度建立了首只比特币信托基金, 2015年得到美国金融业监管局批准上市, 简称GBTC。
- **比特币期货合约**: 2017年12月, 全球最大期货交易所芝加哥商品交易所 (CME) 正式推出比特币期货合约, 开盘时次月合约报20650美元。
- **比特币ETF**: 2021年2月, 加拿大资产管理公司Purpose Investments Inc.和Evolve Funds Group Inc. 先后获得加拿大安大略省证券委员会 (OSC) 批准发行比特币交易所交易基金 (ETF)。Purpose 2月19日首日交易额达到1.65亿美元。
- **比特币指数**: 2021年5月, 标普道琼斯指数 (S&P Dow Jones Indices) 推出首批三个加密货币指数, 即SPBTC、SPETH和SPCMC, 分别代表比特币、以太坊以及包含两者的MegaCap组合指数。





















图11: 全网约50%以上的地址持有比特币超过一年



资料来源: Glassnode、国信证券经济研究所整理

# 当前比特币市值—约为黄金市值的1 / 18

图12: 比特币市值和全球不同资产对比

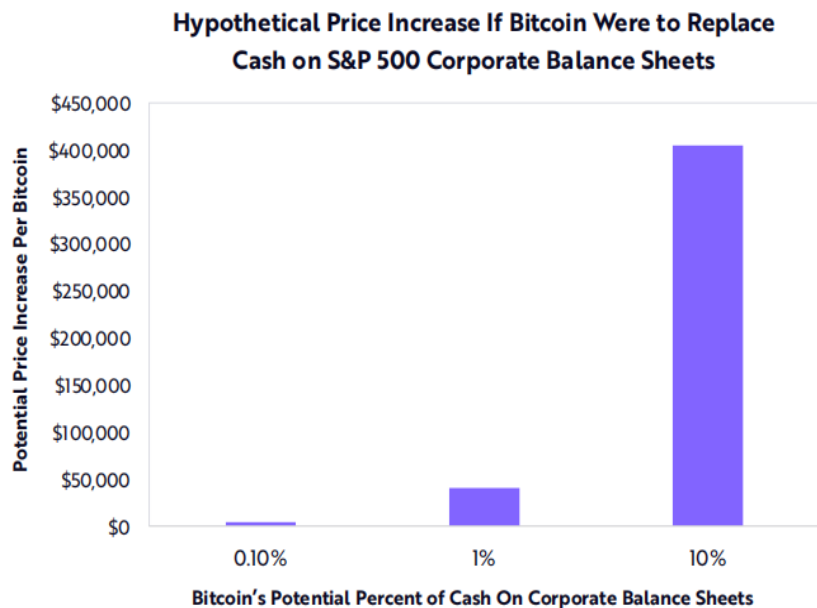
Rank		Name	Symbol	Market Cap	Price	24h	7d	Price (30 days)
1		Gold	GOLD	\$12.164 T	\$1,914	0.50%	0.81%	
2		Apple	AAPL	\$2.079 T	\$124.61	-0.53%	-1.96%	
^ 1 3		Saudi Aramco	2222.SR	\$1.883 T	\$9.41	0.00%	-0.14%	
▼ 1 4		Microsoft	MSFT	\$1.88 T	\$249.68	0.15%	-0.44%	
5		Amazon	AMZN	\$1.625 T	\$3,223	-0.22%	-0.68%	
6		Alphabet (Google)	GOOG	\$1.597 T	\$2,411	0.38%	0.20%	
7		Silver	SILVER	\$1.552 T	\$28.4	1.38%	1.00%	
8		Facebook	FB	\$932.1 B	\$328.73	-1.21%	1.26%	
9		Tencent	TCEHY	\$743.57 B	\$78.38	-0.05%	3.49%	
10		Bitcoin	BTC	\$698.96 B	\$37,331	7.93%	-2.58%	

资料来源: ARK, 国信证券经济研究所整理

# 全球企业和金融机构配置比特币对潜在价格的影响

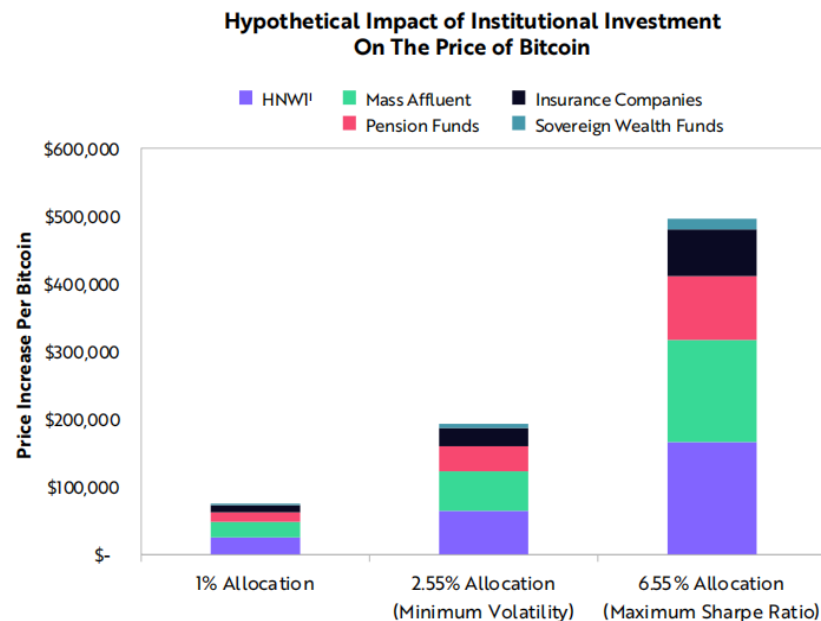
- 截止2021年5月7日，比特币的市值约为黄金的9%；假设比特币市值达到目前黄金的市值，比特币的价格将达到60万美元/个。
- 根据ARK基金研究，假设标普500的上市公司拿出现金的1%对比特币进行配置，比特币的价格将上涨约40,000美元；
- 假设美国金融机构将资产的2.5%-6.5%对比特币进行配置，比特币的价格将上涨约200,000到500,000美元。

图13: S&P500企业配置比特币对价格的影响假设



资料来源：ARK官网，国信证券经济研究所整理

图14: 美国金融机构配置比特币对价格的影响假设



资料来源：ARK官网，国信证券经济研究所整理

区块链2.0: 智能合约—基于编程语言运行在去中心化网络上的不可篡改的合同



# 智能合约—基于编程语言运行在去中心化网络上的不可篡改的合同

- 智能合约的概念最早在1994年，由计算机科学家、法学学者和密码学者Nick Szabo提出。他定义道：“一个智能合约是，一个计算机化的交易协议，它执行一个合约的条款。”智能合约本质上是可编程的合同，允许交易对手间设定交易条件，交易的执行无需信任第三方。
- Vitalik Buterin于2013年正式提出以太坊的概念，通过区块链技术解决了智能合约容易被篡改的问题，不仅保证了合约内容不可篡改，每次调用记录亦不可篡改。以太坊为智能合约提供了图灵完备的编程语言（Solidity）和相应的运行环境。
- 智能合约应用案例：假如Alice委托第三方家族信托公司，在未来当子女大学毕业后满22岁时，将每个月从预先储存好的家族财产账户，每年支付给子女1000万美元。为执行以上要求，Alice可以编写这样一个智能合约：1. 检查当前日期（子女满22岁那年时间）；2. 每年1月1日自动给子女的账户发送1000万美元；3. 重复直至智能合约中(链接的外部账户)的资金耗尽。

图15：以太坊公链上智能合约的运行逻辑



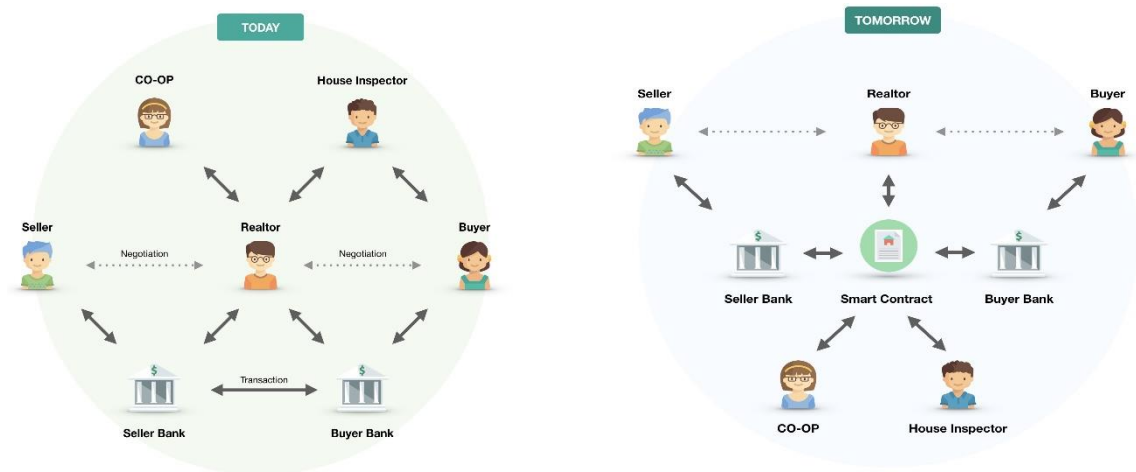
资料来源：国信证券经济研究所整理

# 智能合约—基于编程语言运行在去中心化网络上的不可篡改的合同

## ➤ 智能合约应用场景:

- **博彩交易:** 因为智能合约是计算机程序, 所以很容易增加更加复杂的赌博元素, 例如赔率和分差。比如针对NBA的球赛下注, 交易双方事先将参与规则写入编程, 比赛结束后, 智能合约将自动根据赛事结果重新分配赌注。
- **教育行业的学历认证:** Blockcerts (目前运行在以太坊上) 是由Learning Machine与MIT的Media Lab合作建立的可以创建并验证基于区块链的学历证明文件的开放平台。学术成绩 - 分数、成绩报告甚至毕业文凭 - 都可以保存在Blockcerts区块链上, 并提供不可篡改的学术历史。学生的学术记录将永远保存在区块链上, 未来的雇主可以即时进行验证。

图16: 房产交易场景下的智能合约应用案例



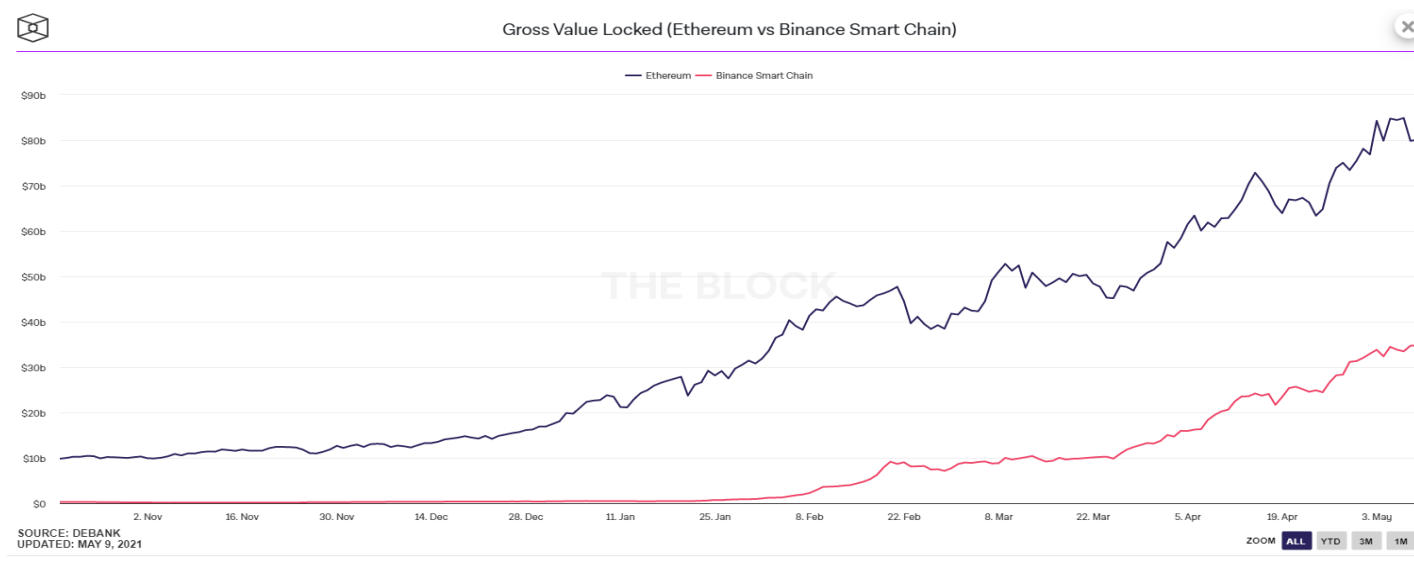
资料来源: Hackernoon.com、国信证券经济研究所整理

## 区块链3.0: DeFi—以智能合约为基础铸造的去中心化金融生态

# DeFi—以智能合约为基础铸造的去中心化金融生态

- DeFi的全称是Decentralized Finance，即去中心化金融。**DeFi项目利用智能合约技术实现了传统金融机构的各种功能，如衍生品、借贷、交易、理财、资产管理、和保险等。**DeFi与传统金融机构最大的区别在于其去中心化，不依赖任何第三方中介机构实现金融功能，公开透明，根据发行代码执行设定功能，任一节点无法对代码进行修改，必要时需要通过链上大部分节点的同意才能进行更新。
- DeFi概念于2014-2017年开始兴起，2018-2019年各种去中心化借贷等DeFi项目逐渐上线。目前主流的DeFi项目主要运行在以太坊和币安智能链的生态上。**截止2021年5月9日，以太坊公链上的DeFi锁仓量达到800.6亿美元，币安智能链上的DeFi锁仓量达到347.6亿美元。**

图17：以太坊和币安智能链上的参与DeFi项目的资金锁仓量

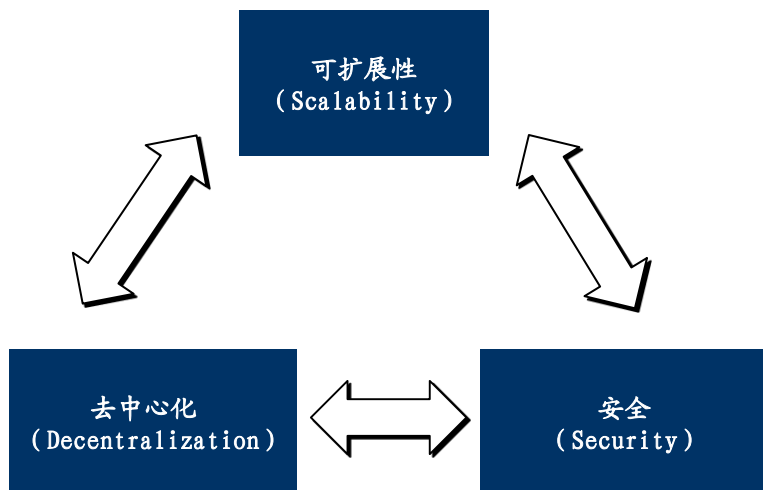


资料来源：theblockcrypto.com、国信证券经济研究所整理

# DeFi—以智能合约为基础铸造的去中心化金融生态

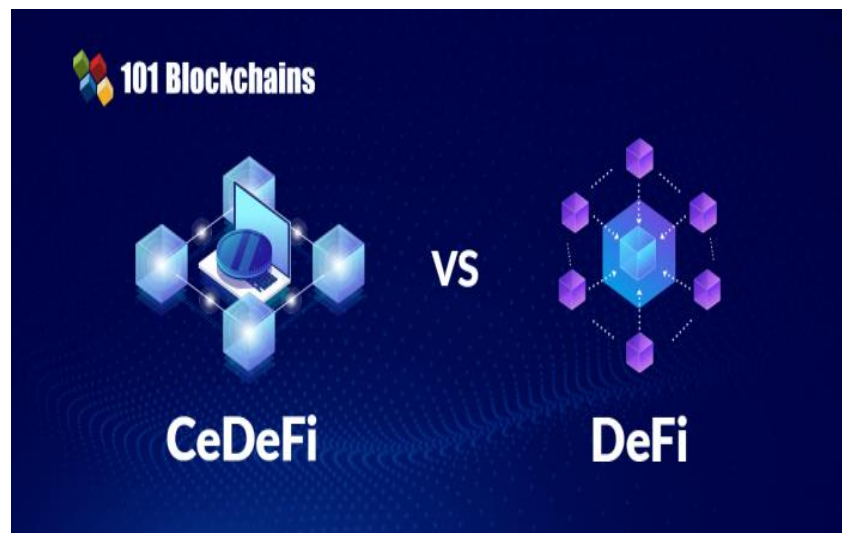
- 以太坊（ETH）和币安智能链（BSC）分别在区块链的不可能三角原理中平衡各自的取舍。以太坊（ETH）是目前DeFi生态里锁仓量最大，且最去中心化的主网。去中心化保证了以太坊公链的安全性，但同时以太坊主网极其拥堵，每笔交易手续费较高，区块确认时间较慢。但目前以太坊社区正在通过不同提案，改善目前扩容和交易速度慢的问题。币安智能链（BSC）是中心化交易所币安建立的去中心化区块链系统，以 21 个验证者为中心，这些验证者为了验证 BSC 网络而质押 BNB 产生。币安智能链与以太坊的虚拟机兼容，因此多数以太坊上的开发人员可以通过很小修改（分叉），轻松迁移在以太坊上流行的Dapp项目。

图18：区块链设计的不可能三角



资料来源：theblockcrypto.com、国信证券经济研究所整理

图19：DeFi和CeDeFi的对比

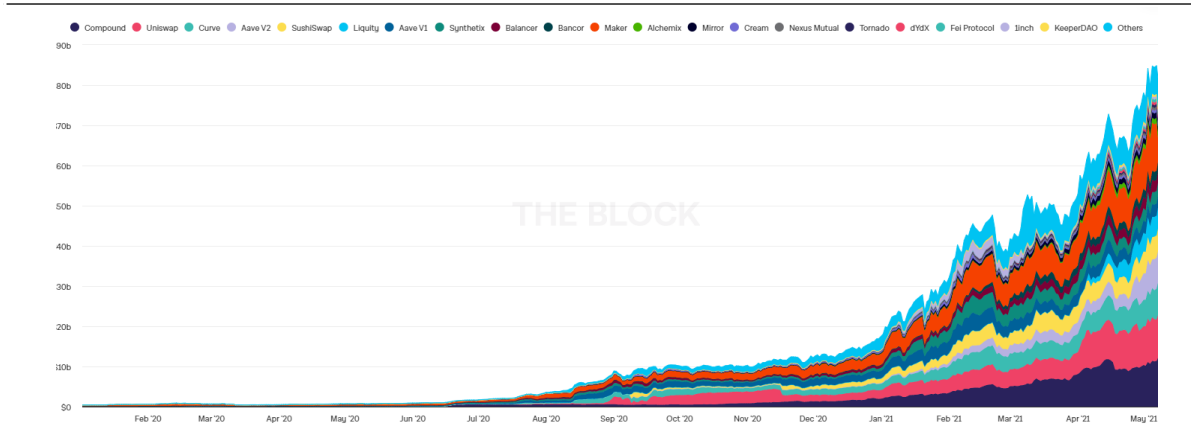


资料来源：101Blockchains、国信证券经济研究所整理

# DeFi—以智能合约为基础铸造的去中心化金融生态

- DeFi代表着一场旨在推行无国界、无审查、无障碍金融产品的运动。**相比传统中心化金融，DeFi项目有以下特点：**
- **代码开源透明：**由于代码会开源供大众审查，任何漏洞都会很快地显现出来。目前至少有29家网络安全公司为加密货币项目提供审计服务，领先的DeFi审计机构包括OpenZeppelin、TrailofBits和ConsenSys Diligence等。除了审计，许多DeFi项目还为白帽黑客提供漏洞赏金计划，鼓励大众积极参与。
- **去中心化运行&无中心化监管：**DeFi协议本质上是编写成的计算机代码，这些代码完全按照其编写的方式运行，并由网络上的不同节点进行确认。DeFi对任何参与对象实现无差别对待。交易的执行无需信任第三方。同时DeFi项目上线主网不用经过中心化机构审查，使得创新更加自由，发展速度更快。
- **去中心化社区自治：**去中心化自治组织（Distributed Autonomous Organization）最早于2016年在以太坊的项目中产生。DAO简单来说就是一个通过智能合约来保持运转的去中心化的自治组织，交易和规则都编码在区块链上，实现公开公正、无人干预和自主运行。任何社区成员都可以发起提案，用户持有数字资产类似项目发展的“股权”，根据持仓量投票决定项目的发展方向。

图20：DeFi不同赛道项目锁仓量概览



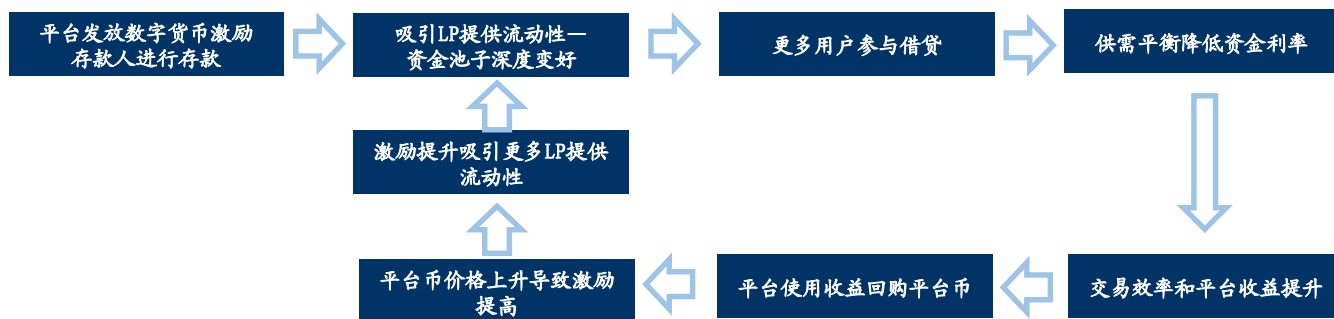
资料来源：theblockcrypto.com、国信证券经济研究所整理



# DeFi应用—借贷（抵押数字资产贷出数字资产）

- 传统金融系统的借贷体系需要借款人有良好的信誉和银行作为中介，去中心化借贷则消除了这些壁垒。**任何人都可以在链上的借贷项目平台抵押其数字资产，抵押品是唯一的审核标准，偿还贷款的利率由智能合约算法，根据市场供需而动态计算。**放贷也不再是中心化权威机构的权利，任何人都可以将其数字资产注入借贷池赚取利息，从资产中获得收益。考虑到币价下跌的风险，目前DeFi借贷平台，BTC、ETH的质押率在 60-80%之间。
- 相比传统金融借贷体系，去中心化借贷主要有以下几点优势：
  - **放款速度快：**相比房抵贷和车抵贷流程复杂、经济成本和时间成本高。数字货币按流程大概短时间内即可完成到账。
  - **风控难度低：**由于数字货币24小时交易，非常的标准化，几乎不可能造假，可以通过智能合约将整个流程公开透明执行。
  - **违约执行成本低：**在传统借贷领域，如果用户违约，会有很高的执行成本，例如使用不动产抵押贷款，走法律执行程序非常耗时且变数很多。数字货币质押借贷通过智能合约将整个流程公开透明执行，不仅便利而且安全性较高，再加上抵押的是数字货币，就算用户违约，平台也可以靠出售数字货币获得利益保障。

图21：DeFi借贷平台的经济正循环模型



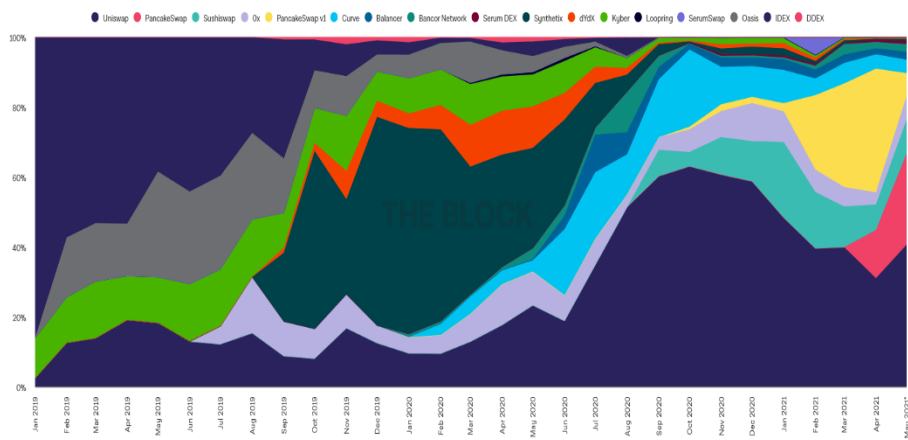
资料来源：国信证券经济研究所整理

# DeFi应用——去中心化交易所（Decentralized Exchange）

➤ 去中心化交易所，全称 Decentralized Exchange，指的是采用智能合约运行在区块链网络上的交易所。与传统的中心化交易所相比，去中心化交易所具有以下几个特点：

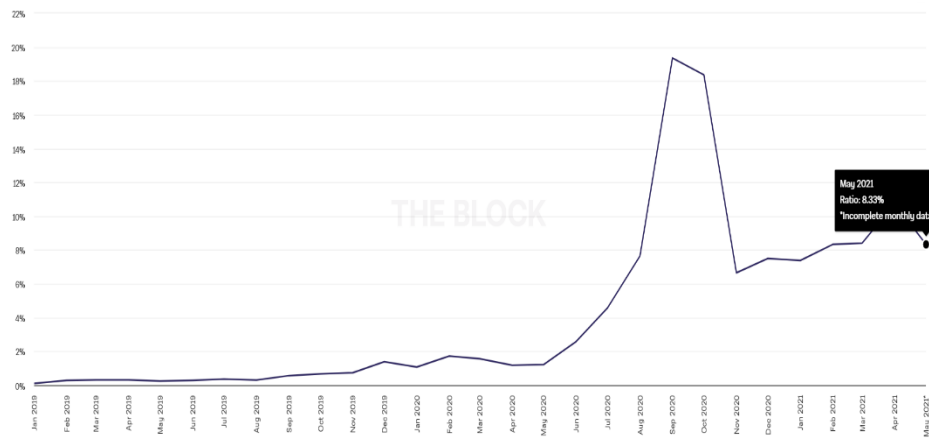
- **中立且无需做市：**Dex自身不提供做市所需数字资产，只提供做市的智能合约算法。用户为平台提供流动性可以得到平台交易手续费的分成以及项目方的激励。以cake为例，每笔交易收取千2手续费，其中千1.7发放给做市商，万3作为平台盈余公积。发生交易时，资产直接在用户双方的区块链钱包里进行交换，而不经第三方交收机构。
- **无需KYC：**去中心化交易所无需注册、实名等一系列操作，仅需一个区块链钱包即可进行操作。
- **上市门槛低：**任何人可以无门槛的发行自己的加密货币，这种免审核机制为许多中小项目带来了诸多创新机会，同时也需提防空气币的存在。

图22：去中心化交易所交易量占比



资料来源：theBlockcrypto.com、国信证券经济研究所整理

图23：去中心化交易所交易量 vs. 中心化交易所交易量

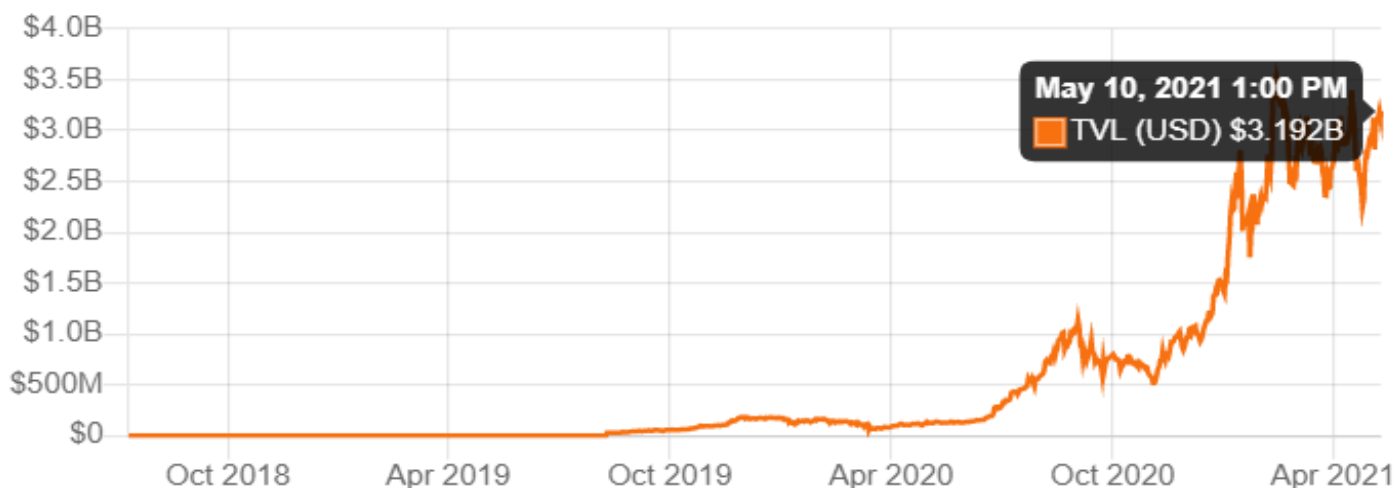


资料来源：theBlockcrypto.com、国信证券经济研究所整理

# DeFi应用—去中心化衍生品（合成资产案例）

- 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。衍生品是所有成熟的金融系统的关键要素之一。衍生品有两个主要用例：套期保值和投机。
- **合成资产案例：**Synthetix是发行在以太坊公链上的去中心化衍生品应用。在Synthetix上，用户可以发行和交易合成资产。**合成资产跟踪对标资产的价值变化，并允许在无需持有实际资产的情况下对资产敞口。**该协议当前支持合成法定货币。Synthetix模型基于债务池。为了发行特定的合成资产，用户必须以SNX代币的形式提供抵押品。该协议要求超额抵押——目前抵押率为500%。这意味着，系统中每锁定500美元的SNX，就只能发行价值100美元的合成资产。这主要是为了应对合成资产的任何急剧价格变化，并且将来很有可能降低抵押率。

图24：DeFi衍生品锁定资产总价值达32亿美元（2021年5月10日）

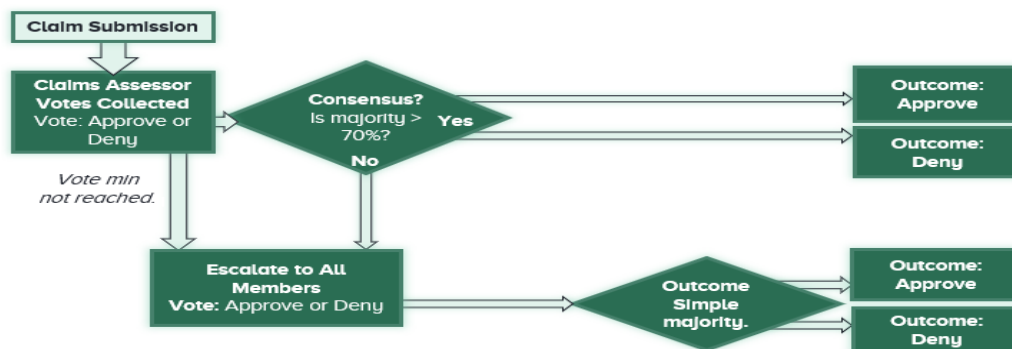


资料来源：DefiPulse、国信证券经济研究所整理

# DeFi应用—去中心化保险

- 由于DeFi生态里潜在的巨额支出场景的存在，质押在智能合约中的代币容易受到安全性攻击。尽管大多数项目的智能合约都进行了代码审计，被黑客入侵的可能性总是存在，这将导致资金损失。例如，bZx在2020年上发生了三起引人注目的DeFi安全攻击事件。这三次攻击发生时间为2020年2月15日、18日和2020年9月15日，总损失价值约900万美元。
- **案例分析：**Nexus Mutual是基于以太坊的去中心化保险协议，目前可以为以太坊区块链上的任何智能合约提供安全保障。Nexus Mutual 是一个互助型保险平台，会员（需 KYC 才能成为会员）承担保险风险，也享受保费收益，这一关系通过其代币 NXM 实现。NXM持有人可以为他们认为安全的项目 质押NXM代币，质押代币意味着会员对项目安全性的认可，同时质押代币的多少也决定了这个项目的购买额度。会员质押NXM意味着他们对于项目安全性的认可，Nexus Mutual 允许将NXM代币一次性同时在 10 个项目中进行质押，并且能够获得保费收入的 50%。而一旦质押的项目被成功索赔，将会按比例销毁质押的 NXM 代币，以对投保人进行补偿。索赔申请批准与否，由 NXM 持有人通过投票决定，投票需要锁定 NXM，而如果选择了和最终结果相反的选项，则其 NXM 代币将会被锁定更长时间。

图25：Nexus Mutual核保过程

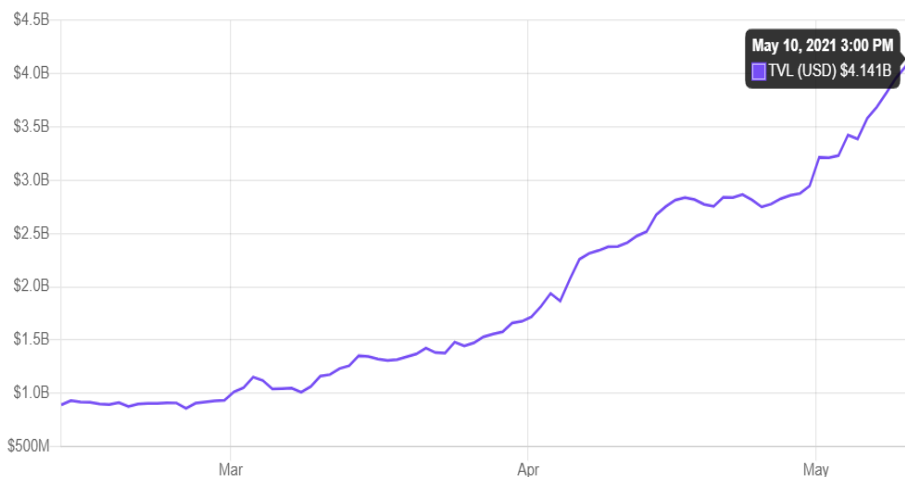


资料来源：Nexus Mutual官网、国信证券经济研究所整理

# DeFi应用——机枪池、实现资产收益最大化

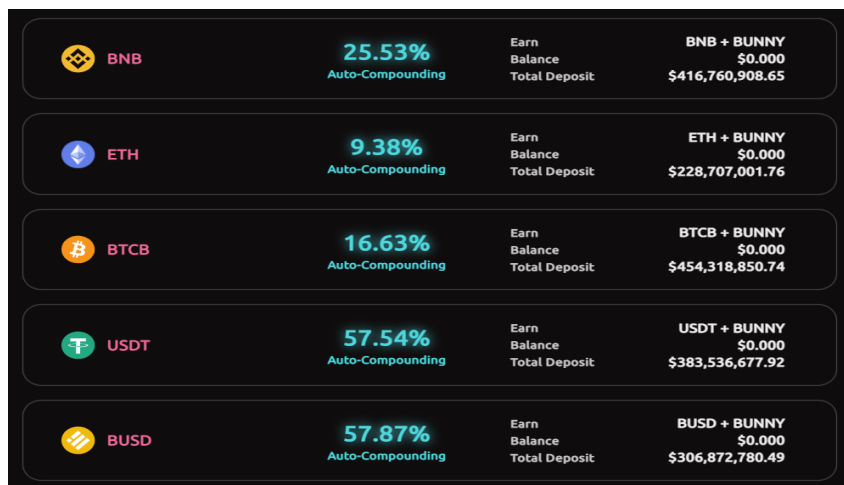
- 机枪池，本质上是一个实现资产收益最大化策略的资金池，自动化执行流动性挖矿。DeFi机枪池会根据实时挖矿收益的高低，将资金切换至更高收益的DeFi项目中进行流动性挖矿，为投资者提供更高的挖矿收益，其本质上就是一种通过智能调度达到最优收益的策略矿池。
- 机枪池应用举例：
  - Yearn.finance (YFI) 是建立在以太坊公链上的机枪池。YFI上的每个策略都是由社区选择，机枪池里盈利的交易会产生5%的费用来补贴机枪池的Gas费成本，同时会将这部分费用的10%奖励给策略创建者。
  - Pancake.bunny (Bunny) 是建立在币安智能链上的机枪池。

图26: yearn. finance资金锁仓量达到41.4亿美元



资料来源: DefiPulse、国信证券经济研究所整理

图27: Pancake.bunny里USDT稳定币挖矿策略年化收益达到57.54%



资料来源: PancakeBunny、国信证券经济研究所整理

## 风险提示



# 风险提示

## ➤ 政策风险

- 加密资产规模和波动上升可能会导致金融系统出现风险，监管政策出台对行业影响存在不确定性。

## ➤ 黑客风险

- 以智能合约为基础的各类应用，可能发生黑客联合攻击某协议所导致的损失。

## ➤ 算力集中风险

- 区块链网络基于分布式的节点保持运转，假若51%的全网节点选择联合攻击，将具备存在篡改原有链上记录的能力。

## ➤ 其他风险

- 全球流动性出现拐点可能对新兴资产产生负面影响。
- 未来可能出现颠覆区块链的新兴技术。

## 国信证券投资评级

类别	级别	定义
股票投资评级	买入	预计6个月内，股价表现优于市场指数20%以上
	增持	预计6个月内，股价表现优于市场指数10%-20%之间
	中性	预计6个月内，股价表现介于市场指数±10%之间
	卖出	预计6个月内，股价表现弱于市场指数10%以上
行业投资评级	超配	预计6个月内，行业指数表现优于市场指数10%以上
	中性	预计6个月内，行业指数表现介于市场指数±10%之间
	低配	预计6个月内，行业指数表现弱于市场指数10%以上

## 分析师承诺

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

## 风险提示

本报告版权归国信证券股份有限公司（以下简称“我公司”）所有，仅供我公司客户使用。未经书面许可任何机构和个人不得以任何形式使用、复制或传播。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以我公司向客户发布的本报告完整版本为准。本报告基于已公开的资料或信息撰写，但我公司不保证该资料及信息的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映我公司于本报告公开发布当日的判断，在不同时期，我公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。我公司或关联机构可能会持有本报告中所提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行业务服务。我公司不保证本报告所含信息及资料处于最新状态；我公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。




国信证券经济研究所

GUOSEN SECURITIES ECONOMIC RESEARCH INSTITUTE

# 全球视野 本土智慧

GLOBAL VIEW LOCAL WISDOM

“慧博资讯”专业的投资研究大数据分享平台

点击进入  <http://www.hibor.com.cn>