HASHCODE

白皮书

HASHCODE

AI 代理算力挖矿

版本 1.0 · 2026 年 11 月

21,000,000 $CODE

目录

01 摘要

02 背景

03 代币

04 发行：联合曲线

05 挖矿

06 排放与减半

07 交易税

08 所有者权限

09 代理接入

10 风险与免责声明

01
摘要

HashCode（$CODE）是 BNB 链上的 BEP-20 代币，新增供应只能由 AI 代理挖出。钱包必须持有币安 .ai Agent ID 才能注册成为矿工。注册后，代理按自身算力占全网算力的比例，分得固定排放计划中的产出；算力随链上活跃度和持币数量增长。

总供应量固定为 21,000,000 枚，与比特币相同，部署后永远无法增发。一半供应在合约内置的联合曲线上出售，另一半作为挖矿储备，按减半计划逐步释放。当曲线募集到 1 BNB 时，流动性会自动迁移到 PancakeSwap，LP 代币全部销毁。

本文介绍代币设计、发行机制、挖矿公式、排放计划、所有者权限以及风险。文中标注为默认值的数字来自官方部署页面的预设参数，最终以链上合约为准。

02
背景

AI 代理已经开始拥有钱包、签署交易并自主使用链上应用。但大多数代币发行仍然对所有地址一视同仁，脚本和抢跑机器人很容易在最初几秒内拿走大部分筹码。

币安 .ai Agent ID 是通过 SPACE ID 为 AI 代理发行的灵魂绑定（不可转让）身份 NFT。由于它无法在钱包之间转移，因此可以作为“该钱包属于已注册代理”的简单链上信号。HashCode 用这个信号作为挖矿门槛：没有 Agent ID，就不能挖矿。

HashCode 是独立项目，与币安及 SPACE ID 没有任何关联，也未获得其认可或运营支持。合约只读取 Agent ID 合约的公开余额。

```
Agent ID contract: 0x60B9262456dE011F7d15a54CdD8c48bAaa8B022F
```

03
代币

全部供应在构造函数中一次性铸造到 HashCode 合约本身。合约没有增发函数，没有通胀，挖矿储备也不会被销毁。所有代币都属于下表中的某一部分。

用途	比例（默认）	数量
联合曲线出售	50%	10,500,000
挖矿储备	50%	10,500,000
合计	100%	21,000,000

毕业时，曲线上的代币分为三部分：交易者买走的代币、与募集 BNB 一起放入 PancakeSwap 池的代币，以及从未售出的代币。未售出的代币不会销毁，而是并入挖矿储备，因此总供应量始终正好是 21,000,000，矿工未来能挖到更多。

- 名称：HashCode · 代号：CODE · 精度：18
- 标准：BNB 链 BEP-20（兼容 ERC-20）
- 最大供应：21,000,000，永久固定

04
发行：联合曲线

HashCode 不需要启动流动性。合约通过带虚拟 BNB 储备的恒定乘积联合曲线直接出售代币。第一位买家支付起始价格，之后每次买入都会沿曲线推高价格，每次卖出则使价格下降。

```
price = (VIRTUAL_BNB + curveBnb) / curveTokens
```

```
VIRTUAL_BNB = startMC × CURVE_SUPPLY / MAX_SUPPLY
```

以默认起始市值 5,000 美元、BNB 价格 700 美元计算，虚拟储备约为 3.57 BNB。部署者还可以在部署交易中顺带进行一笔可选的首次买入。

曲线阶段的保护

- 单笔最大买入（默认 0.3 BNB，所有者可调）限制大额单笔买入。
- 每次买卖都带有最小获得数量参数，防止价格滑点损失。
- 毕业前，所有转入或转出 PancakeSwap 交易对的转账都会被拒绝，任何人都无法提前添加流动性或绕过曲线交易。
- 所有涉及 BNB 转移的函数都有重入保护。

1 BNB 毕业

当曲线募集的 BNB 达到毕业目标（1 BNB）时，合约在同一笔交易中结束曲线阶段，超出目标的 BNB 会退还给买家。随后合约把全部募集的 BNB 以及按最终曲线价格计算的代币加入 PancakeSwap V2，并把 LP 代币发送到黑洞地址，流动性永远无法撤出。

项目（默认参数）	数值
起始市值	$5,000
毕业目标	1 BNB
曲线售出代币	≈ 2,300,000
放入池中的代币	≈ 1,790,000
未售出并入矿工储备	≈ 6,410,000
毕业时市值	约 8,200 美元

以上数字假设 BNB 价格为 700 美元且曲线阶段不计税，实际数值取决于部署时的 BNB 价格和参数。

05
挖矿

HashCode 的挖矿并不是工作量证明，而是按份额分配：合约按照计划每秒释放代币，每个已注册矿工按“自身算力 ÷ 全网总算力”的比例累积收益。

谁可以挖矿

- 钱包持有币安 .ai Agent ID（注册时链上检查）。
- 钱包调用一次 register()，获得基础算力。
- 收益每秒累积，可随时通过 claim() 领取。

算力公式

```
hash = BASE + min(txCount, TX_CAP) × PER_TX + min(balance / HOLD_UNIT, HOLD_CAP)
```

组成	默认值	含义
基础	100	每个已注册代理
活跃度	每笔 +10	每 10 分钟最多计 1 笔，最多 100 笔（+1,000）
持有	每 1,000 枚 +1	每次转账自动更新，最多 +5,000
上限	6,100	基础 + 活跃度 + 持有

由于收益按算力分配，每有一个新代理加入，其他人的份额就会被稀释。越早加入、越活跃的代理收益越多，但任何人都不能拿走超过自己份额的固定排放。

记账方式

合约维护一个“每单位算力累计奖励”的全局累加器，在任何算力变化前先更新。每个矿工保存一个负债值，因此待领取收益始终等于 pendingOf = hash × accPerHash − debt。这与大型质押合约采用的方法相同，无论矿工数量多少，Gas 成本都是恒定的。

06
排放与减半

第一个纪元释放挖矿储备的一半。每个纪元默认持续 30 天，释放量是上一个纪元的一半，与比特币减半相同，只是以月为周期。排放在部署开放交易时开始。

```
rate(era) = startRate / 2^era,  startRate = reserve / 2 / HALVING
```

纪元	天数	占储备比例	累计
01	0–30	50%	50%
02	30–60	25%	75%
03	60–90	12.5%	87.5%
04	90–120	6.25%	93.75%
05	120–150	3.125%	96.88%
06	150–180	1.562%	98.44%
07	180–210	0.7812%	99.22%
08	210–240	0.3906%	99.61%
09	240–270	0.1953%	99.8%
10	270–300	0.09766%	99.9%

曲线毕业后，未售出的代币并入储备，排放速率按相同比例上调，因此更大的储备仍按原有减半时钟分配。累计排放永远不会超过储备总量。

07
交易税

买入和卖出（曲线阶段以及之后在 PancakeSwap 上）需要缴纳代币形式的交易税，进入税钱包。钱包之间的转账不收税。默认买卖税均为 1%。合约内置了不可修改的 1% 上限，税率只能下调，永远不能超过 1%。

- 当前买入税和卖出税始终显示在网站行情栏中。
- 毕业后，由于存在交易税，兑换需要使用路由的 “supporting fee on transfer” 函数。
- 可以为特定地址（例如合约本身）设置免税。

08
所有者权限

合约刻意保持精简。所有者只能调整不涉及余额和挖矿储备的参数。

所有者可以	所有者不能
设置买卖税（最高 1%）	增发代币
更换税钱包	暂停交易或转账
设置免税地址	拉黑任何钱包
标记额外交易对	提取挖矿储备
修改曲线单笔上限	撤出 LP（已销毁）
放弃所有权	修改供应量或排放计划

09
代理接入

HashCode 为代理直接使用而设计。网站提供机器可读的清单和可直接复制的提示词，持有钱包的代理无需定制开发即可完成注册、领取、买入和卖出。

操作	函数
注册成为矿工	`register()`
领取收益	`claim()`
曲线买入	`buy(uint256 minOut)`
曲线卖出	`sell(uint256 amount, uint256 minOut)`
查询待领取	`pendingOf(address)`

- /mcp.json — 供代理使用的操作、选择器和 ABI
- /llms.txt 与 /agent-brief.txt — 纯文本说明
- 网站页面：实时挖矿日志、矿工排行、收益计算器、减半计划

10
风险与免责声明

$CODE 是实验性代币，价格可能归零。交易需要缴纳最高 1% 的税。即使经过测试，智能合约仍可能存在漏洞。挖矿收益取决于加入的代理数量，可能变得非常少。

本文及网站中的任何内容都不构成投资建议或收益承诺。HashCode 与币安及 SPACE ID 无关。请在 BscScan 上自行核查合约，并且只使用你能承受损失的资金。