# 矿币，新时代的淘金热

专题报告　　行业研究

2019.09.11

通证通研究院
区块链研究报告


通证通研究团队
分析师：宋双杰，CFA
Email: master117@bqbase.org

分析师：程东锋
Email:chengdongfeng@bqbase.org


更多研究请关注通证通公众号获取

请务必阅读最后特别声明与免责条款

**导读：**BTC 诞生 10 年来高达百万倍的涨幅造就了人类金融史上的一个传奇，其他与 BTC 相似的矿币争相走向加密市场的舞台，接受市场的检验，上演着一幕幕新时代的淘金热。


**摘要：**

**矿币是基于 POW 共识机制，通过算力“挖矿”获取通证的通证种类。**最早的矿币 BTC 诞生于 2009 年，是整个加密世界的“开山鼻祖”，十年来高达百万倍的涨幅造就了人类金融史上的一段传奇。**从 2019 年年初到现在，BTC 网络算力不断攀升并创下历史新高，当前 BTC 全网的运算速度相当于 66 台世界上运算速度最快的计算机。**

**受财富效应刺激，其他矿币“你方唱罢我登场”，在加密市场的舞台上轮番表演，但大多数已被市场所淘汰。**

矿币是加密市场的重要成员，目前市值排名前 50 的通证中，矿币占有 14 个席位，占比 28%，市值排名前五的通证中有 4 个都是矿币。

2018 年年末到 2019 年年初，加密市场遭遇寒冬，投资者纷纷转战市值较小的矿币。**矿币之所以能在熊市得到投资者青睐，一般来说是因为矿币无预挖、技术强、估值较低、社区自治。**同时矿币有专门的矿机进行挖矿，可以让熊市中的投资者锚定出一个成本价格。矿币的风险在于初期市场流动性较差。

市值排名靠前的矿币除了 Decred（DCR）采用 POW 和 POS 的混合挖矿机制，其余矿币都采用 POW 共识机制——节点获得记账权的概率与该节点拥有算力的比例相关。

Bit Asset Chain 设计了一套新型的矿币系统，建立了一套具有通缩属性的 POS 经济系统，模拟 BTC 挖矿的经济模型，包含 BCV 和 BAC 双通证。BCV 为 Bit Asset Chain 的权益通证，用于竞选生态节点时的抵押和投票。生态节点负责 Bit Asset Chain 记账、出块和治理等服务，并会获得实用型通证 BAC 作为奖励。Bit Asset Chain 的 ZI-POS 模型，克服了 POW 能源浪费和效率较低的固有缺陷，同时通过通缩的双通证模型来保障通证持有者的权益，模拟出 BTC 挖矿的经济模型，但能否得到市场认可，尚需时间检验。

风险提示：共识机制漏洞

# 目录

# 图表目录

# 1 矿币简史

## 1.1 矿币始祖 BTC

**矿币是基于 POW 共识机制，通过算力“挖矿”获取通证的通证种类。**所谓“挖矿”是将网络协议规定的获取通证的方式类比为物理世界的“淘金”或“挖矿”。

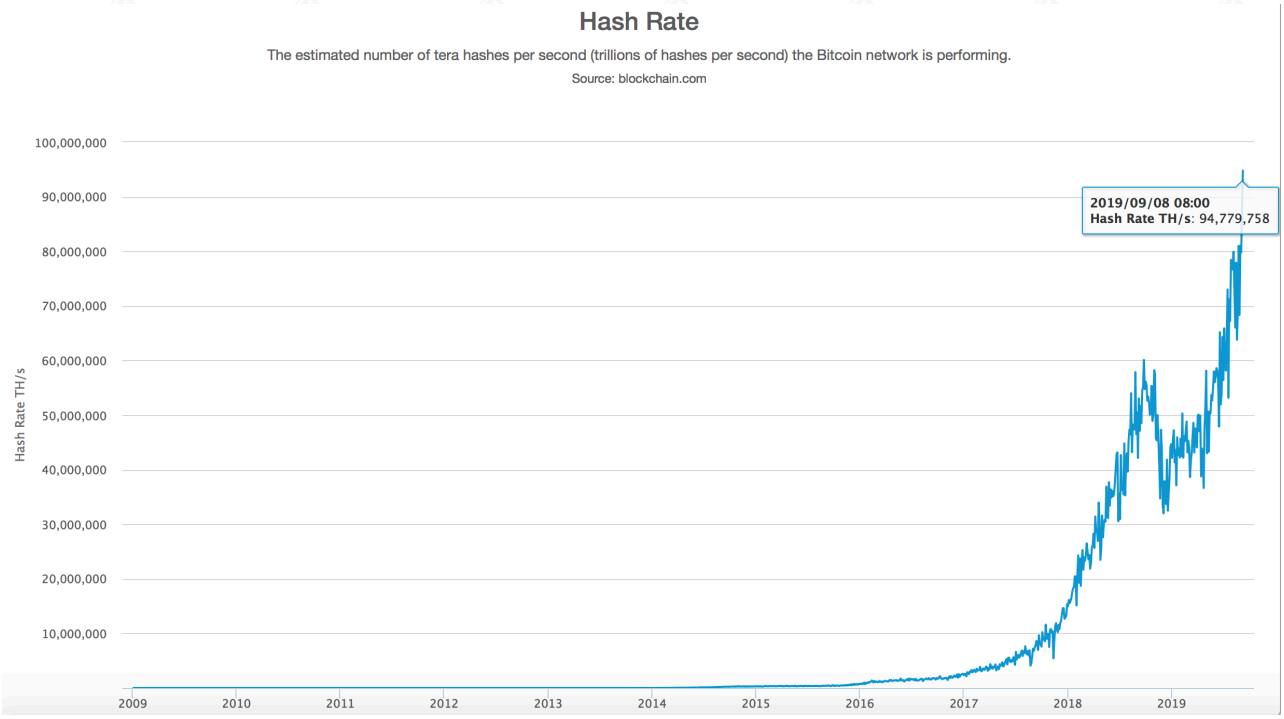
**最早的矿币 BTC 诞生于 2009 年，是整个加密世界的“开山鼻祖”，十年来高达百万倍的涨幅造就了人类金融史上的一段传奇。**

BTC 基于区块链技术，是一种点对点的电子现金系统，为避免通胀问题，规定总量是 2100 万枚。网络节点通过争夺记账权的方式获取 BTC 奖励，BTC 网络协议规定“挖矿奖励”每 4 年减半一次。

BTC 神秘创始人中本聪的最初愿景是人人都可以使用自有算力参与到 BTC 的挖矿中来，但后来由于财富效应的驱使，专业的强算力矿机投入到“军备竞赛”中来，甚至逐渐衍生出由专业矿机组成的挖矿“军团”——矿池。

blockchain.com 数据显示，从 2019 年年初到现在，BTC 网络算力不断攀升，并于 9 月 8 日再创历史新高，逼近 95 EH/s。根据 2018 年 11 月世界 Top500 超级计算机榜单最新报告，世界上运算速度最快的计算机是美国 IBM 研发的 Summit，运算速度为 143.5 亿亿次，中国天河-2A 超级计算机运算速度是 61.44 亿亿次，排名第四。当前 BTC 全网的运算速度相当于 66 台 Summit，154 台天河-2A。

图表1：BTC 全网算力变化趋势图




*资料来源：blockchain.com，通证通研究院*

## 1.2 早期的“竞争”矿币

**受财富效应刺激，其他矿币“你方唱罢我登场”，在加密市场的舞台上轮番表演，但大多数已被市场所淘汰。**例如 2011 年诞生的矿币 Ixcoin、Tenebrix、Solidcoin 都已走向凋零：IxCoin 几乎复制了 BTC 的所有特征，只不过区块奖励更多；Tenebrix 试图抵制 GPU 挖矿；Solidcoin 的区块产生速度更快，这三种通证都有预挖矿（即创始人在一开始就拿走大量矿币）。2011 年诞生的矿币经过大浪淘沙，目前只剩下没有预挖矿的 Litecoin 和 Namecoin。2013 年排行较为靠前的矿币大多也都销声匿迹。

图表2：2013 年 5 月加密市值排行

| # | 币种名称 | 符号 | 市值 | 币价 |
|---|---|---|---|---|
| 1 | Bitcoin | BTC | $1,261,032,047 | $113.46 |
| 2 | Litecoin | LTC | $61,100,879 | $3.53 |
| 3 | Namecoin | NMC | $5,710,684 | $1.05 |
| 4 | Peercoin | PPC | $5,596,144 | $0.297292 |
| 5 | Feathercoin | FTC | $2,532,299 | $0.400646 |
| 6 | Freicoin | FRC | $2,109,841 | $0.107150 |
| 7 | Terracoin | TRC | $1,349,993 | $0.562622 |
| 8 | Devcoin | DVC | $1,208,631 | $0.000275 |
| 9 | Novacoin | NVC | $971,890 | $3.53 |
| 10 | Mincoin | MNC | $170,594 | $0.166895 |

*资料来源：CoinMarketCap，通证通研究院*

Litecoin（LTC）借鉴 BTC 于 2011 年创立，作出了一定的参数调整，总量 8400 万枚（BTC 是 2100 万枚）。LTC 每 2.5 分钟产生一个区块（BTC 是 10 分钟），与 BTC 相比交易确认速度更快。LTC 首创了 Scrypt 加密算法，与 BTC 的 SHA256 算法相比，更有利于普通计算机的挖矿。

Bytecoin（BCN）不是简单复制 BTC 代码，而是第一个基于 CryptoNote 技术的数字通证，主打“匿名支付”的牌。BCN 诞生于 2012 年，目前在加密市场仍然占有一席之地。

Infinitecoin（IFC）定位于日常生活的小额支付，诞生于 2013 年 6 月 5 日，由几个美国黑客所创，采用 Scrypt 算法，每 30 秒生成一个区块，每生成 86400 个区块挖矿奖励减半。2013 年 8 月，IFC 一度冲到加密市场市值排行榜前十，然而一年后随着 906 亿枚 IFC 几乎被全部挖出，区块奖励接近 0，全网算力锐减，逐渐被市场抛弃。

Dogecoin（DOGE）诞生于 2013 年 12 月，最初基于网络的草根文化、小费文化而设计，通过巧妙的营销活动取得了较大的成功，在虚拟通证领域拥有仅次于 BTC 的用户数量和非中心化程度。虽然是模仿 BTC 设计，但市场认可度较高，2019 年 4 月、7 月，DOGE 先后上线 Huobi、Binance 等知名交易所。

图表3：部分早期矿币一览

| 矿币种类 | 通证符号 | 发行时间 | 当前总市值 |
|---|---|---|---|
| Bitcoin | BTC | 2009 | 1849 亿美元 |
| Litcoin | LTC | 2011 | 45 亿美元 |
| Bytecoin | BCN | 2012 | 0.8 亿美元 |
| Infinitecoin | IFC | 2013 | -- |
| Primecoin | XPM | 2013 | 360 万美元 |
| Zetacoin | ZET | 2013 | 27 万美元 |
| Dogecoin | DOGE | 2013 | 3 亿美元 |
| Monero | XMR | 2014 | 13 亿美元 |
| Dash | DASH | 2014 | 8 亿美元 |

*资料来源：CoinMarketCap，通证通研究院*

## 1.3 矿币现状

**矿币是加密市场的重要成员，目前市值排名前 50 的通证中，矿币占有 14 个席位，占比 28%，市值排名前五的通证中有 4 个都是矿币。**

图表4：加密市值 50 强中的矿币

| 矿币 | 市值排名 | 共识机制 | 核心算法 | 发行年份 | 标签 |
|---|---|---|---|---|---|
| BTC | 1 | POW | SHA256 | 2009 | 支付类 |
| ETH | 2 | POW/POS | Ethhash | 2015 | 公链类 |
| BCH | 4 | POW | SHA256 | 2017 | 支付类、公链类、分叉通证 |
| LTC | 5 | POW | Scrypt | 2011 | 支付类 |
| BSV | 9 | POW | SHA256 | 2018 | 支付类、公链类、分叉通证 |
| XMR | 10 | POW | CryptoNight | 2014 | 支付类、匿名通证 |
| DASH | 15 | POW | X11 | 2014 | 支付类、匿名通证 |
| ETC | 17 | POW | Ethhash | 2016 | 公链类、分叉通证 |
| ZEC | 29 | POW | Equihash | 2016 | 支付类、匿名通证 |
| DOGE | 30 | POW | Scrypt | 2013 | 支付类 |
| DCR | 32 | POW/POS | BLAKE256 | 2016 | 支付类 |
| BTG | 38 | POW | Equihash | 2017 | 支付类、分叉通证 |
| RVN | 41 | POW | X16R | 2018 | 支付类、公链类 |
| BCD | 49 | POW | X13 | 2017 | 支付类、分叉通证 |

*资料来源：CoinMarketCap，通证通研究院*

**2018 年年末到 2019 年年初，加密市场遭遇寒冬，投资者纷纷转战市值较小的矿币。**例如主打快捷支付的 Turtlecoin（TRTL）、基于 MimbleWimble 隐私协议的 Grin（GRIN）和 Beam（BEAM）、主打资产上链功能的 Ravencoin（RVN）都在这一时段内实现了数倍的涨幅。

**矿币之所以能在熊市得到投资者青睐，一般来说是因为矿币无预挖、技术强、估值较低、社区自治。同时矿币有专门的矿机进行挖矿，可以让熊市中的投资者锚定出一个成本价格。矿币的风险在于初期市场流动性较差。**

# 2 典型矿币分析

## 2.1 匿名通证的新星——GRIN/BEAM

MimbleWimble 是一种增强区块链隐私性和性能的区块链协议，能够在不存储整个区块链历史记录的情况下，验证所有交易是否有效。MimbleWimble 的主要特点有：

1）隐私性。通过盲因子将交易发送方、接收方和转账金额等信息隐藏起来，但是可以验证链上的通证总输入等于总输出。

2）扩展性。MimbleWimble 只存储未使用的 UTXO，可以节省账本空间并加快同步速度。

Grin 是第一个使用 MimbleWimble 底层协议的项目，主网于 2019 年 1 月 16 日上线，GRIN 开始面世正式成为匿名通证家族的一员。Grin 无 Crowdsale、无预挖矿，由社区驱动，在精神层面接近于 BTC 的原教旨，受到 BTC 核心开发成员等人的追捧。Grin 的区块奖励恒定为每分钟 60 枚 GRIN，通证总量无上限。

Beam 同样也是基于 Mimblewimble 的匿名通证项目，和 Grin 相比，Beam 为公司化运作，通证总量为 2.628 亿枚，并且在最初的 5 年内，区块奖励的 20%进入开发者财政库。

图表5：GRIN/BEAM 与其他主流矿币对比

| 矿币 | 发行时间 | 是否 Crowdsale | 是否预挖矿 | 分配方式 | 市值排名 |
|---|---|---|---|---|---|
| BTC | 2009.01 | × | × | 每四年减半，总量 2100 万枚 | 1 |
| ETH | 2014.07 | √ | √ | 预挖 7200 万枚，后续每年增发 1800 万枚 | 2 |
| LTC | 2011.01 | × | × | 每四年减半，总量 8400 万枚 | 5 |
| XMR | 2014.04 | × | × | 总量 1840 万枚，2022 年开采完成后每年固定发行少量通证 | 10 |
| DASH | 2014.01 | × | × | 挖矿速度先快后慢；总量 1890 万枚，前 24 小时挖出 190 万枚；区块奖励的 45%归矿工 | 15 |
| ZEC | 2016.10 | × | × | 前 20000 个区块的奖励线性递增到 12.5 个，正常出块后每四年减半；前四年区块奖励的 20%归团队，80%归矿工 | 29 |
| DOGE | 2013.12 | × | × | 1000 亿枚挖矿结束后，每年增发 50 亿，总量无上限 | 30 |
| BCN | 2012.07 | × | √ | 固定时间区块奖励减半，预挖 80%以上 | 59 |
| BEAM | 2019.01 | √ | × | 最初五年区块奖励的 20%归开发团队，80%归矿工，总量 2.628 亿枚 | 89 |
| GRIN | 2019.01 | × | × | 每分钟出一个区块，区块奖励恒定为 60 枚，总量无上限 | 91 |

*资料来源：各项目官网，通证通研究院*

## 2.2 过山车一样的 Turtlecoin（TRTL）

Turtlecoin 的愿景是成为一款易于使用的支付类通证，通过使用轻区块（Lite Blocks）来进行节点之间的同步。轻区块和完整的区块相似，但只包含交易的哈希值，而不包括交易的输入、输出、签名

等内容。轻区块大小只有完整区块的 1%，可以显著减少网络节点需要传输的数据量，缩短传输时间。

Turtlecoin 特性如下：

1）高 TPS。Turtlecoin 的出块速度是 20 秒，是 BTC 的 30 倍。

2）隐私性。采用和 XMR 一样的环签名技术保护隐私。

3）易于挖矿。支持 CPU 挖矿。

4）社区运营。无预挖，无融资。

Turtlecoin 的通证 TRTL 在 2019 年 1 月份和 4 月份先后两次冲击价格高点，热闹一时，但目前回到了最初的价格，价格走势如同过山车。2019 年 9 月 10 日 CoinMarketCap 上的市值排名仅为 718 名。

图表6：TRTL 的市场表现


*资料来源：CoinMarketCap，通证通研究院*

## 2.3 红极一时的 Ravencoin（RVN）

Ravencoin 是于 2018 年 1 月 3 日在 BTC 的基础上创立的具有特定用例的区块链网络：将资产（包括黄金等实物资产和 BTC 等数字资产）从一方转移到另一方，主网于 2018 年 8 月 31 日正式推出，通证 RVN 总量 210 亿枚，目前流通量约为 43.9 亿。

Ravencoin 以资产为中心，在 Ravencoin 系统内，资产可以是黄金、股票、游戏道具、数字通证等实物资产或虚拟资产。例如黄金上链的项目可以在 Ravencoin 上发行黄金资产，定义资产通证的总量，并可进行相互交易。

Ravencoin 的资产用 ID 进行唯一标识，每进行一次资产注册需要消耗一定量的 RVN。如果 RVN 社区和应用逐步发展壮大，资产 ID 将具有稀缺性。

2018 年 10 月 11 日，知名通证交易所 Binance 创始人赵长鹏发布一则 Ravencoin（RVN）即将在币安上线的推文，力挺 RVN，RVN 一周内暴涨 3 倍。

Ravencoin 没有 Crowdsale，没有预挖，创始团队没有预留，社区自治。Ravencoin 在 BTC 的基础上创立，但是与 BTC 相比有如下区别：

1）区块奖励： BTC 初始区块奖励为 50 枚，而 RVN 为 5000，之后都是每四年减半；

2）出块速度： BTC 是 10 分钟，RVN 为一分钟；

3）通证总量：BTC 总量为 2100 万枚，RVN 为 210 亿；

4）挖矿算法： BTC 采用 SHA-256 哈希算法，而 RVN 采用 X16R，该算法可防止 ASIC 矿机挖矿，从而让更多人可以参与进来，更好地实现非中心化。

进入 2019 年以来 RVN 再度发力，2 个月内上涨 600%，成为 2019 年上半年上涨幅度最大的通证之一。

## 3 新型矿币系统——无通胀 POS 共识机制

前文所讨论的矿币除了 Decred（DCR）采用 POW 和 POS 的混合挖矿机制，其余矿币都采用 POW 共识机制——节点获得记账权的概率与该节点拥有算力的比例相关。

POW 共识机制的缺陷在于，会造成大量的资源浪费，且网络性能较低。POS 共识机制是通过所谓“权益”在网络中占比来争夺记账权，它的出现源自人们对 POW“算力竞赛”中消耗大量能源的批判。**但 POS 本身也存在一定问题，其中之一便是其固有的通胀模型会不断稀释通证持有者的权益。**

Bit Asset Chain 是基于区块链技术打造的数字资产管理平台，通过对 POS 共识机制进行改良，设计出 ZI-POS（Zero Inflation Prove of Stake，0 通胀 POS）经济模型，实现对 BTC 挖矿机制的拟合。

**具体来说，Bit Asset Chain 建立了一套具有通缩属性的 POS 经济系统，设计了包含 BCV 和 BAC 的双通证系统。BCV 为 Bit Asset Chain 的权益通证，用于竞选生态节点时的抵押和投票。生态节点负责 Bit Asset Chain 记账、出块和治理等服务，并会获得 BAC 通证奖励。**

BAC 除了是生态节点的奖励通证以外，Bit Asset Chain 链上转账、智能合约运行、数据存储等操作均需要消耗 BAC。

图表7：Bit Asset Chain 双通证系统

| 通证名称 | 通证类型 | 通证作用 |
|---|---|---|
| BCV | 权益型通证 | 竞选生态节点锁仓和抵押、用户投票 |
| BAC | 实用型通证 | 生态节点奖励、运行智能合约等 |

*资料来源：通证通研究院*

锁定 BCV 进行挖矿，获取的区块奖励是 BAC 通证。BAC 的总量恒定为 4400 万枚，同样也有区块奖励减半机制。Bit Asset Chain

五秒钟出一个块，每半年减半一次，初始区块奖励为每天 144,000 枚 BAC。

此外 BAC 会不断被销毁，用户在 Bit Asset Chain 的转账矿工费、运行智能合约的 GAS 费会全部销毁。为配合销毁机制，Bit Asset Chain 设计出了一套能量值模型。BAC 的通缩模型有助于增加通证稀缺性，可能刺激通证价格上涨。

**Bit Asset Chain 的 ZI-POS 模型，克服了 POW 能源浪费和效率较低的固有缺陷，同时通过通缩的双通证模型来保障通证持有者的权益，模拟出 BTC 挖矿的经济模型，但能否得到市场认可，尚需时间检验。**

附注：

因一些原因，本文中的一些名词标注并不是十分精准，主要如：通证、数字通证、数字 currency、货币、token、Crowdsale 等，读者如有疑问，可来电来函共同探讨。

## 免责声明

本报告由通证通研究院提供，仅供本公司客户使用。本报告仅在相关法律许可的情况下发放，所提供信息均来自公开渠道。本公司尽可能保证信息的准确、完整，但不对其准确性或完整性做出保证。

本报告的完整观点应以通证通研究院发布的完整报告为准，任何微信订阅号、媒体、社交网站等发布的观点和信息仅供参考，本公司不会因为关注、收到或阅读到报告相关内容而视相关人员为客户。

本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，相关的分析意见及推测可能会根据后续发布的研究报告在不发出通知的情形下做出更改，投资者应当自行关注相应的更新或修改。

市场有风险，投资需谨慎。本报告中的信息或所表述的意见仅供参考，不构成对任何人的投资建议。投资者不应将本报告为作出投资决策的唯一参考因素，亦不应认为本报告可以取代自己的判断，本公司、本公司员工或者关联机构不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告中的任何内容所引致的损失负责。



本公司对本免责声明条款具有修改和最终解释权。