FREECASH

自由现金

自 由 演 进 的 密 码 货 币

（V0.2.2，2019.7.29）

二〇一九年七月

目录

1 为什么发布自由现金

密码货币是全新的货币形态，它能克服现行法币体系的通货膨胀、中介成本和汇兑成本等缺陷，为互联网经济提供内生价值循环系统，成为全球市场通用的货币。

1980 年代末开始，Timothy May、David Chaum、Dai Wei、Adam Back、Hal Finney 等人就提出或试验基于非对称密码和互联网技术构建隐私的、去中介的密码货币。经过 20 年的尝试和失败，直到 2008 年中本聪发布《比特币：一种点对点的电子现金系统》，利用经前人发展的一系列技术，构建了高度去中心化的比特币系统。经过 10 年运行，比特币的基本构架被证明具有很强的生命力，为密码货币的成功奠定了坚实的基础。

然而，货币形态的演化是一个长期过程。最早的铸币出现于 2700 年前，取代它的可兑换纸币出现于 1000 年前，而不可兑换纸币出现于 300 年前，电子货币从 1960 年代出现至今， 80 年过去了仍没有完全取代纸币。从法币体系到密码货币也是一个长期的演进过程。

尽管很多人认为比特币足够伟大，能够成为唯一成功的密码货币。但随着密码货币的发展，越来越多的人改变看法，并且尝试了各种新的方向：

2012 年出现了基于 PoS 共识机制的点点币；

2014 年诞生了基于 DPoS 的 BTS；

2015 年出现了专注智能合约的以太坊；

2015 年区块链概念兴起，无代币区块链应用起步；

2016 年比特币拥堵，扩容之争白热化；

2017 年比特币区块扩容失败，市值从 90%跌至 40%，爆发 ICO 浪潮和公链大战；

2017 年比特币分裂为定位数字黄金的 BTC 和定位电子现金的 BCH；

2018 年 BCH 遭遇比特币原教旨主义攻击，后者失败后分裂出激进扩容的 BSV。

这一系列事件证明，密码货币是一个探索的过程，伴随市场规模和影响力的不断扩大，其技术、经济与社会生态系统会越来越复杂，新的问题会不断涌现。目前看来，去中心化密码货币在共识机制、开发中心化、算力中心化、方向分歧、路线分歧、理念分歧、性能与安全权衡、去中心社区治理等方面都面临挑战。

这些挑战表明，密码货币的成功不是一条笔直的大道，中本聪只是打开了一扇门，前方道路还需要我们不断开拓和选择。自由现金是基于比特币与比特币现金框架所做的一项试验性探索。

2. 自由现金的定位

自由现金的发展目标是：**自由演进的去中心化电子现金系统。**将在发展中坚持以下原则：

2.1 分工：专注点对点电子现金

结构、功能与性能紧密相关，适当的结构保障功能以更高性能实现，多种功能的集成不仅提高结构复杂性带来风险，还会因功能的相互影响降低性能。去中心化的自然界和市场经济总是通过分工和协作逐渐进化出复杂而稳定的生态，去中心化的密码经济也应如此。

在比特币与以太坊的分裂中，比特币为电子现金设计的账户结构、数据结构、确认时间等不适合复杂的智能合约，而以太坊智能合约的复杂性则降低了系统的稳定性，货币功能受到制约。超越密码经济发展阶段，做结构复杂、功能多样、性能卓越的全能系统是不可能成功的。

因此，自由现金定位为**简单易用的点对点电子现金**，专注做去中心化的通用货币，主要通过市场机制与其他密码应用形成协作，在分工协作中成为未来密码经济的一部分。

2.2 继承：延续历经时间检验的比特币基础框架

比特币是经历了 10 年时间反复验证，最为成熟稳定的去中心化货币底层框架。扩容之争后，比特币通过隔离见证大幅改变了交易和区块结构，将发展方向从点对点电子现金转换为结算网络，尝试通过闪电网络承接全部支付功能。这种探索还有待时间检验。

自由现金将采取更加保守的发展策略，继承比特币现金的技术框架和演进主义发展理念。这样不仅技术上较为安全，也能够最大程度上复用比特币和比特币现金长期积累的基础设施，降低用户进入门槛。

自由现金构想始于 2017 年初，当时扩容之争暴露了中本聪框架无法解决的开发中心化问题，比特币现金通过分叉暂时解决了扩容问题，但治理框架没有改变，分叉又带来新的挑战。船大难掉头，比特币现金对基础性改进很难达成社区共识。自由现金作为新生系统，将为比特币现金的进化提供试验田，成为进化中的比特币生态的组成部分。

2.3 **演进：针对新问题不断改进。**

货币是复杂的社会经济系统，新货币形态需要经历长期，逐步发现问题做适应性改进。中本聪在之前 20 年密码货币探索基础上建立比特币，此后 10 年比特币也不断面临新的问题，远远超出中本聪个人的能力范围，是去中心化的构架帮助比特币在 10 年内，在中本聪中途隐退的情况下，汇集各方智慧逐步发展壮大。

比特币 10 年在中本聪框架的基础上主要解决了所遇到的一系列技术问题，2014 年之后的分歧分裂暴露出的更多是经济、政治、文化层面的问题，尚未形成新的解决机制。自由现金主要针对这些问题，对中本聪框架做出谨慎、简洁的调整，尝试解决这些问题，使其更加利益相容、决策高效、文化和谐。

幸运的是，密码货币已经呈现出百花齐放的竞争局面，自由现金不需要再造轮子，在演进中可

以借鉴各种竞争币经过市场检验的方案和技术，并由简入繁，不断探索适应市场需求的技术和机制改进。

2.4 参与：降低门槛并提供激励

去中心化是密码货币的灵魂。货币是经济的枢纽，它太重要以至于不能依赖于特定个人或组织，中心将集中承受巨大的利益冲突和经济波动，单点失败的系统风险巨大。这是比特币之前各种密码货币失败的主要原因。目前，最可靠的中心化货币是货币当局管理的法币体系，也普遍面临持续通胀、汇兑成本和货币政策干扰市场等问题，这正是比特币出现的原因。

因此，自由现金将深化比特币开创的去中心化方向，在生态的各个领域鼓励和吸引更多人参与。借助比特币与比特币现金的技术框架和基础设施，降低了解、应用和开发自由现金的技术门槛；通过建立新链的方式，降低获得和使用自由现金的经济门槛。自由现金还将借助内生的贡献基金对贡献者予以经济激励，形成可持续的公共参与支持。

2.5 高效：提高进化和决策效率

比特币两次分叉和中心化密码货币兴起暴露了去中心化面临的主要问题：公共决策难度大、效率低。主要体现在：

1）当发生重大分歧的时候难以协调。如比特币扩容之争延续超 2 年，区块拥堵 1 年后才以分叉告终。

2）在公共事务处理中搭便车现象严重。比如 BCH 社区早期对比特大陆的过度依赖。

3）信息不对称和专业门槛导致共识难以达成。比特币扩容之争和 BCH 版本之争中，多数人无法理清技术差异、路线差异和背后的理念分歧，很难做出理性判断。

4）当面临有组织的社会攻击的时候难以组织有效防御。如 nChain 借 BCH 硬分叉升级时机，展开精心筹划的攻击，给 BCH 生态造成重大损失。

自由现金通过新币奖励的方式形成贡献基金，在此基础上，建立社区治理结构和治理协调组织，探索去中心化社区的有效治理结构，提高公共决策效率，在竞争环境中实现高效的系统进化。

2.6 自由：实现自由协作与自由竞争

“自由”是人类的终极目标，马克思与哈耶克都追求自由，只是认定的路线不同。自由现金的灵魂也是“自由”，它以去中心化的方式实现自由协作，以分叉共存的方式实现自由竞争。

自由现金的本质是市场经济的内生货币，它：

1）专注于电子现金功能，与其他功能的密码应用通过市场形成分工协作；

2）借助中本聪框架和贡献基金实现利益相容和系统内自愿协作，自由进出，同时保障决策效率；

3）对重大分歧通过分叉实现对不同方向，或以不同方式探索演进，通过市场自由竞争，实现优胜劣汰，适者生存。

通过自由协作和自由竞争，自由现金将逐步探索实现货币自由的道路，为构建全球自由密码经济体系做出努力。

3 自由现金的特征

自由现金的发展是一个长期演进的过程，基于密码货币的发展经验和自由现金的定位，自由现金的第一个版本（FreeCash v1）具有以下特征：

3.1 命名与单位

自由现金的英文名称为 FreeCash，缩写为 FCH；

货币单位采用“ƒ”，即“freecash”首字母，发音可简化为“fesh”，中文发音“飞士”；

小额支付常用单位取小数点后第六位，货币单位记作“¢”，即“cash”首字母，读“cash”，中文发音“开士”；

最小货币单位（小数点后第 8 位）为纪念中本聪仍采用比特币的单位“satoshi”，按习惯中文读作“聪”；

3.2 Schnorr 签名

Schnorr 签名被公认为是比椭圆曲线签名更加高效，扩展性更强的签名算法。BTC 预计将在 2020 年上线 Schnorr 签名。BCH 在 2019 年 5 月 15 日升级中已经实现了 Schnorr 签名。但是 BTC 和 BCH 都必须继续支持椭圆曲线签名算法，以保证原有交易的合法性，这将增加系统的复杂性和拓展 Schnorr 签名应用的难度。FreeCash 作为一个新链，将放弃椭圆曲线签名，全面采用 Schnorr 签名。

3.3 POW 共识机制

工作量证明共识机制（PoW）经过 Adam Back 和 Hal Finny 的探索改进，由中本聪成功应用于比特币。它以十分简洁的方式解决了货币的去中心化记账、公平发行和安全交易，是密码货币从早期探索走向成功的关键。比特币 10 年运行验证了它的可靠性。自由现金也将采用中本聪框架的工作量共识机制。

3.4 SHA256 算法

以往出现的 POW 密码货币为了避免比特币 SHA256 挖矿算法巨大算力的 51%攻击威胁，往往更换挖矿算法，如莱特币改为 scrypt 算法。重组保护的加入消除了 51%攻击威胁，使得自由现金可以继续采取 SHA256 挖矿算法，从而更好地利用比特币和比特币现金长期积累形成的挖矿基础设施。

3.5 1 分钟确认

比特币的工作量证明机制设置了 10 分钟的平均出块时间，这是依据 2008 年前后的网络和运算设备状况制定的。目前的硬件条件能够更快传输和验证区块，因此可以缩短。目前已经有 Doge、Grin 等采取了 1 分钟出块，提供更好的用户体验并稳定运行。自由现金经过测试也采取 1 分钟出块时间。

3.6 防重组保护

POW 面临的最大威胁是 51%攻击重组区块链，造成双花损失和市场恐慌。2018 年 11 月的 BCH 算力大战中，BCH 遭遇公开、持续、有组织的 51%攻击威胁，最终通过加入 10 个区块重组保

护的方式成功化解，取得算力大战的胜利。为此，自由现金设置 30 个区块重组保护，防范 51%攻击，这也使大额转账 30 分钟可确保安全。

3.7 逐块调整难度

由于中本聪框架下，挖矿难度每 2016 个块（约两周）调整一次，在同一个挖矿算法运行多个链时，算力会全部涌入相对收益较高的链，导致该链频繁出块，而另一个链则无法出块。难度调整后算力反涌。这种情况下，小链无法生存。为此，比特币现金将挖矿难度调整为逐块调整（DAA）解决了这个问题，自由现金继承了这种算法。

3.8 无预挖无众筹

治理基金将从每个区块持续产出，解决公共资金需求，因而不需要预挖，也不需要代币众筹（ICO）。预挖和 ICO 一方面具有法律风险，另一方面当预挖和众筹资金耗尽时，仍将失去资金来源。何况不少预挖币和 ICO 币一开始就是为了套现，先借理想情怀造势，套现之后宣布将币交给社区，留下既无治理基金，又无治理结构的所谓“去中心化社区”。每块产生的治理基金将更持久地保障公共治理资金需求。

3.9 内生治理基金

去中心化社区也需要公共决策，扩容之争反映出中本聪框架公共决策的低效和开发者激励的缺失，BCH 算力大战则反映出缺乏公共决策机制的的去中心化社区面对中心化攻击的脆弱。进行公共决策的一个基本前提要资金用于公共决策和公共事务。为此，自由现金突破中本聪框架，在 coinbase 提供挖矿奖励的同时产生治理基金。

3.10 发行逐年衰减

比特币新币发行每 4 年减半。减半意味着市场上的新币供给减少一半，在需求连续变化的情况下，会对价格造成冲击，形成了明显的 4 年牛熊周期，振幅也较大。自由现金为平滑这种波动，挖矿新币奖励将从每块 25f 开始，每年缩减 20%，治理基金将从每块 25f 开始，每年缩减 50%。挖矿奖励衰减速度较比特币略快，而治理基金则快速衰减，以适应前期运营资金压力较大，后期币价更高的趋势。

3.11 20 年后稳定发行

比特币到 2140 年新块奖励将衰减至 0 ，挖矿全部依赖交易费收益激励。考虑到交易费会随着市场需求产生大幅波动，而比特币扩容失败，区块容量过早被限制，使交易量难以显著增长，交易费难以提供足够的挖矿激励。为了避免这些问题，并提供长期安全和治理的基本资金需求，自由现金将在约 20 年后（12096000 高度）停止衰减。此时每个新块的挖矿奖励为 0.23 f，治理基金约每块 0.000012 f，能够提供稳定的挖矿激励和治理基金。此时货币总量年增长约千分之一，不会产生通货膨胀问题。

3.12 发行总量 1 亿

按照上述发行速度，自由现金将在 20 年内从 0 开始发行总量 1 亿 f。尽管 20 年后将停止衰减，但每年发行速度仅为存量的千分之一，80 年后的总量也仅仅达到 1.08 亿 f。因此可以说，自由现金的发行总量为 1 亿。

4 自由现金的运营

4.1 人员构成

去中心化是密码货币获得持久生命力的源泉，自由现金的运营也是自愿参与这场试验的自愿者的个人行为组合。我们没有固定的团队。理解密码货币、认同自由现金理念的人正在不断加入，也有人因各种原因离开。总体上，正在参与自由现金试验的是注重自由演进的、经验丰富的密码货币参与者，毕竟自由现金的路线跟当前流行的路线有很大差异，理解和认同它并不容易。

这些自愿参与者不打算宣传自己的名字。在一个去中心化密码货币系统中，个人社会身份并不重要，自由现金不需要依赖个人光环，参与者也并不打算借自由现金获得名誉。每个人参与进来是为了做自己认为正确的事情，并可以自愿离开，这是去中心化的基本保障。

自由现金的参与者根据自己的喜好选择是否匿名。大部分参与者并不难找到，也不担心被找到。毕竟，中本聪已经替我们承担了创造一种全新货币体系的绝大部分风险。有人努力证明自己是中本聪，更多人用自己的信用背书发行密码货币，这说明发行新的密码货币不再是危险的事了。自由现金不众筹、不预挖，只是根据每个人的贡献，事后获得自由现金的内生货币激励，这也规避了参与者的个人风险。

在自由现金发展的早期，理解自由现金的人较少，面临的设计开发问题会比较多，同时又很难获得经济回报，因此，需要一些人为了理想相对集中地开发和运营。随着了解和参与的人越来

越多，开发运营将会越来越去中心化。比特币成功的经历也告诉我们，去中心化不是一个状态，而是一个过程。我们力争按照系统发展和市场需求，逐步提高自由现金的去中心化程度，实现自由现金社会价值的安全稳定增长。

4.2 资金来源

即使是去中心化社区，也有公共事务需要处理。去中心化密码货币目前面临的最大问题就是社区公共治理问题，而公共治理资金是解决问题的前提。

比特币的经历，以及历史上许多重要革新的发展经历表明，早期的推动需要有信仰和理想推动，但一旦产生广泛的经济影响，经济利益相容则是革新是否能够存活的关键。比特币扩容之争中开发者缺乏经济激励，从而追求无政府主义理想而不顾市场需求；在 BCH 算力大战中，资金支持下有组织攻击给缺乏公共资金支持，从而难以有效组织的 BCH 社区造成了巨大损失。

自由现金设计的初衷之一就是解决去中心化社区的公共治理问题。为此，在新币发行的挖矿奖励之外，设立了治理基金，以最简单的方式解决了公共治理资金问题，完善中本聪框架的经济激励相容机制。

在自由现金早期，即使是新币发行奖励也由于缺乏市场估值和交易深度而无法成为真正的经济激励。这一方面借助于参与者基于理想自愿贡献能力、精力和时间，降低系统运行成本；另一方面也接受参与者自愿的资金捐助。

在自由现金系统逐渐稳定，市场有所接受的情况下，自由现金的治理基金发行将会覆盖主要的运营费用。随着市场认可程度的加强，治理基金将达到一个峰值，支持完成自由现金系统和生态的主体构建。自由现金的治理基金将逐年衰减，快速递减，20 年后系统成熟，每年将有 6f 用于支撑系统和生态的日常运营维护。

4.3 基金使用

自由现金的治理基金用于公共支出和激励对自由现金和密码货币的发展做出贡献的人。主要包括开发激励、组织经费和科普经费。

开发激励包括对底层系统的开发和周边应用的开发，包括对经营性开发团队的激励和对志愿和匿名开发者的捐助。对于自由现金开发中参考借鉴的比特币、比特币现金及其他各种密码应用项目，也将从治理基金中支付一些自由现金，以示尊重和感谢。

组织经费用于建立线上和线下社区组织，维护社区公共治理的必要花费，包括协调组织的日常支出，召开会议进行公共决策的费用，社区咨询专家的报酬等。

科普经费用于对自由现金、密码技术、密码货币、密码经济等相关知识的普及和宣传，包括线上线下活动组织、科普网站或工具的开发、自由现金水龙头等。

匿名贡献者是去中心化密码货币创立和发展的重要力量。在去中心化社区中，匿名贡献者基于理想和兴趣所做的工作具有独特价值，是系统安全的最后保障。治理基金将尽力为他们提供支

持，也尊重和赞扬他们不接受任何资助的意愿。

4.4 贡献评估

治理基金的使用机制不影响自由现金系统的安全稳定运行，但会影响社区决策和开发进展，从而影响系统演进。对于去中心化社区的资金管理目前缺乏成熟的模板，需要摸索。自由现金将按照以下原则建立治理基金使用机制：

公开透明原则。公开透明是保证公平和效率的最重要原则。治理基金产生于新币发行，是公开透明的。治理基金的使用和分配也将记录在链上，可追溯，可验证。

事后评估原则。为提高效率，减少分歧和反复，获得资助的活动总体上在活动完成，或阶段性完成的情况下，对活动成果和过程进行评估后给予资助。

专业评估原则。为保证资助效率和公平，对贡献的评估将依据活动本身的特征，选择专业人士展开评估。

民主集中原则。在专业评估基础上，为保证公平将采取民主的方式确定分配方案，但当民主方式效率过低时，治理基金私钥持有者将有最终决定权。

5 加入自由现金试验

作为去中心化密码货币，任何人都可以加入自由现金。作为复杂社会系统，自由现金也需要各领域的专业知识。自由现金将以降低技术门槛、复用成熟基础设施、激励贡献者等方式鼓励各领域人士加入。加入自由现金试验，您可以：

学习密码货币。自由现金与比特币等主流 POW 币种的底层结构相同，可供学习的资料较为全面成熟。而自由现金历史数据极少，容易安装同步，交易费极低，可以低门槛、低成本展开学习和试验。所学知识也很容易拓展到比特币等 POW 主流币以及许多区块链应用。

使用自由现金。在掌握基本知识，能够安全持有和使用私钥的前提下，可以尝试获得和使用自由现金，接受他人支付的自由现金或支付给他人。由于自由现金是从 0 开始的新密码货币，所以使用范围也是从 0 开始，更需要您的使用。熟练使用自由现金也有助于您安全使用比特币和比特币现金等。

开发相关应用。有条件的参与者可以尝试开发自由现金相关的各种应用，这些应用在比特币和比特币现金等密码货币中已经有很多，多数有开源代码，可以非常方便的移植和拓展，这也是一件非常有趣的事情。同样，自由现金的低门槛、低成本也有助于您的开发，开发积累的经验也很容易用到比特币和比特币现金等的应用开发。

尝试新的方向。密码货币还处于早期探索阶段，方向、功能、路线等仍可能出现多种分歧，分

歧的根本原因在于未来的不确定性，需要的市场中慢慢检验。多方向探索和冗余竞争是密码货币生存和壮大的根本动力。自由现金在自由共识的前提下，支持不同方向的探索，珍惜难以消除的分歧，鼓励分叉探索。

总之，自由现金是一块密码货币的试验田，期待与更多热爱自由、坚持理性、追求美好生活的人一起，站在巨人的肩膀上，探索人类更高的自由。

中本聪为我们打开自由之门，我们要继续探索道路。

（FFF，V0.2.2，2019.7.27）