自由共识
freeconsensus

自由共识
为密码经济奠基

自由共识白皮书 1.0

二〇二〇年七月

目录

自由共识是基于中本聪框架演化形成的密码共识系统，是由点对点电子现金系统向密码经济基础设施的进化，从去中心化的自由现金延伸到去中心化的身份、关系、信誉、协议、存储等领域，为密码经济奠基。

1. 密码共识

密码共识系统是采用非对称密码技术和分布式共识机制构建的技术经济系统，主要解决信息经济的信息安全和信息垄断问题。

非对称密码技术于 1970 年代产生于军事用途，1980 年代在密码朋克的推动下走向民用化，用于解决网络信息安全，保护个人隐私，主要用于网络通讯和构建数字货币系统，即密码货币。

分布式共识机制的本质是简单民主机制，即按照多数人认同的规则和判断行事。世纪之交，Napster、BitTorrent 等点对点网络技术的出现，为通过网络在全球范围内建立分布式共识系统提供了技术条件。

2007-2009 年，中本聪发现，早期密码货币纷纷失败的根源是系统的“中心化”。为此，他将分布式共识机制用于密码货币，建立了第一个去中心化的密码货币——比特币。

中本聪用非对称密码技术与分布式共识机制建立的比特币系统，既是一个技术系统，也是一个重要的经济系统。它让素不相识的人们基于私利即可自觉维护一个至关重要的经济系统——世界货币。

我们将这个系统框架称为“密码共识”，即“非对称密码+分布式共识”。它以非对称密码保障信息安全，以分布式共识消除中心垄断，因此，能够用于信息经济基础设施构建。区块链只是分布式共识机制用到的数据结构之一，不能充分体现密码共识的性质和意义。

2 自由现金

比特币是第一个密码共识系统，基础的经济模型满足了早期发展需求。但在 2013 年前后进入主流经济之后，其经济模型开始面临严峻的考验，矛盾在 2015-2017 年的扩容之争中全面爆发。

扩容之争中暴露的主要问题包括：1）开发者缺乏内生激励；2）缺乏有效的治理机制；3）开发者和矿工非专业决策经济政治问题；4）严重分歧导致高成本分叉。

这些问题的出现表明，比特币的确是一场伟大的试验，随着密码共识系统相关社会经济实践的深入展开，系统需要在经济、政治、社会等层面上继续演进，不断成长完善。

遗憾的是，比特币社区多数人没能看到问题，比特币也已经成为庞大的经济体，缺乏高效的治理机制，难以敏捷地进化。这导致扩容失败，比特币的核心功能从点对点电子货币，转向了价值存储的数字黄金。

比特币现金实现了扩容，继承了点对点电子货币方向，并为生存而演进。修改了难度调整算法，增加了重组保护。但仍然难以解决开发者激励、社区治理、专业决策和高成本分叉等问题。

在继承比特币现金演进成果的基础上，为了解决这些问题，自由现金改进了中本聪框架：

1）增加了每区块的治理基金发行，用治理基金激励包括开发者在内的各领域建设者；

2）所有建设者共同参与贡献的事后博弈评估，实现按贡献分配；

3）各领域建设者依据贡献大小获得话语权，实现各领域的专业决策；

4）鼓励重大分歧启动共识分叉，借贡献奖励延时释放，实现分叉各方的利益相容。

自由现金于 2020 年 1 月 1 日 0 点从 0 区块启动，一天内经历 CPU 挖矿、GPU 挖矿、ASIC 矿机挖矿，两个月内实现了矿池、浏览器、钱包、门户等生态设施的多元化，进入了正常运行。

自由现金的治理机制已经完成两期贡献评估，103 个密码身份的 269 项贡献得到奖励。贡献激励机制推动了生态建设者规模的快速增长。对中本聪框架改进的第一阶段取得了成功。

3 密码身份

自由现金的去中心化治理机制要求建设者们以去中心化的身份建设、协作、评估、分配等。中本聪框架作为去中心化货币系统已经提供了去中心化的身份系统，即私钥、公钥和地址体系。

在社区治理中，地址和公钥虽然可以代表身份，但对人类不友好，缺乏社会痕迹，难以记忆。为此，自由现金建立了“密码身份（Crypto Identity，CID）”系统：任何人可以通过链上声明，自定义网名加上地址后四位后缀，形成与地址和公钥一一对应的、全网唯一的密码身份。

CID 包含社会含义，易于识别记忆，加上地址后缀可对应地址，提高安全性，并防止靓号抢注带来的资源垄断寻租行为。

CID 在贡献评估中的应用证明，个人可以独立地使用多个 CID 从事不同活动，每个活动都可以在形成完整的生活闭环。比如，分别以开发者和推广者两个独立身份，分别做事、合作、评估、获得分配、购买或投资等，实现了自由的身份。

CID 不仅可以用于个人的不同身份，也可以代表多人组成的团队，还可以代表某个产品、网站、APP，或者某个设备。它实际上是密码经济中通用的主体身份。自由现金生态已经开始用 CID 在链上注册团队和发布产品。

密码身份系统从自由现金货币系统发展而来，但却是密码经济真正的基石。这个身份系统在中

本聪框架中已经建立，其上才是比特币的货币系统。CID 是在应用中根据需求对中本聪框架身份系统所做的改造，不仅能改进货币系统，还会演化出更丰富的密码经济。。

4 密码关系

一旦建设者们开始用密码身份从事各项活动，密码身份建立相互关系的需求就产生了。这些关系通过私钥签名的方式登记在主链上，就能够建立一个公开可信的密码关系网络，构建密码经济的社会基础。

比如，一个人至少需要两个 CID，一个离线保存私钥，保障重大权益安全，另一个在线保存私钥，方便日常频繁签名。可以将离线 CID 定义为在线 CID 的主控者，一旦在线 CID 私钥泄露，离线 CID 可以声明并转移一些可以转移的权益。

除了单向授权之外，还可以多个 CID 同时签名，在链上声明共同相互关系。比如，3 个 CID 在链上声明相互等同的关系，它们就可以分享所有可执行的权益，从而实现身份的备份。

密码关系的更多场景在于多人之间的授权或契约。比如，贡献评估中，某建设者 CID 可以链上发布声明，委托某评估人 CID 代理其全部的贡献评估事项。评估应用平台将根据这样的链上声明，准许评估人 CID 代理授权人的评估事务。

多个 CID 可以通过链上联合声明建立团队或发布产品（APP 或服务）的方式，建立链上的协作关系和契约关系，或分享发布权。从而建立链上可查、可证、无法篡改的各种复杂的商业关系。

5 开放信誉

基于 CID 和密码关系，有经济意义的活动被记录在链上，可以积累形成开放的信誉系统，为密码经济的商业活动提供依据。

CID 所拥有的自由现金（FCH）数量和链上交易记录是一个重要的信誉指标，可以体现该 CID 的偿付能力，反映其收入和支出状况，为商业合作方提供信誉参考。

中本聪框架所特有的币天（Coin Days，CD）可以用于防止刷单和撸羊毛。任何数量的 FCH 一旦获得，即开始随着时间流逝产生币天，直至被花掉，花掉即销毁币天。以销毁币天为条件可以大幅提高造假成本。自由现金已经在有奖注册 CID 活动和币天奖励活动中成功应用了币天。

贡献奖励的是一个 CID 为生态建设所做贡献的奖励，记录在主链上，能够作为 CID 信誉评价的重要指标。历史贡献越大，奖励越多的 CID 将获得更高的声誉。

CID 之间还可以直接通过链上声明评价其他 CID，也可以对其他 CID 所做的声明或行为（比如贡献声明、产品发布）等进行链上认证。这些评价和认证可以结合主体的信誉增加被评价认证者的信誉信息。

擅长信用评估的机构，可以利用链上的丰富数据构建自己的信誉评价系统，对 CID 的信誉进行评级，并用于商业用途。这种信誉评价能够实现基础数据的完全公开和评级业务的充分竞争，

消除信息垄断，提高社会公信力。

6 自由协议

从中本聪框架开始，去中心化的密码共识系统就是开放的协议系统，任何人都可以自愿遵循协议进入共识。自由现金、密码身份、密码关系也都是通过协议实现的。协议的去中心化决定了密码共识的去中心化。

自由的协议是开放基础设施的前提。自由共识的协议系统完全开放，任何人都可以以自己的方式发布协议。任何人可以用自己的方式采用或实现任何协议。没有任何个人、组织或协议强制实现任何协议。

各种协议在市场上自由竞争，优胜劣汰，演进出相对稳定的协议系统。

新协议出现，需要争取更多的应用采用，越多应用采用，协议的协同优势越大。但是否能够被更多应用采用，最终取决于这些应用能否在市场上获得更多用户。

自由共识系统没有强制机关和强制措施，因此，各种协议可以自由的复制、改进。按照当前的共识，协议应在主链上发布，并署名发布者的 CID。

任何人可以改进任何已经发布的协议，发布为自己署名的协议，只需要标注出引用的协议。这样采用者可以追溯协议的来源，并且订阅各级发布者的更新信息，便于理解、信任和采用协议。

7 分层共识

在从自由现金扩展到更多去中心化设施的过程中，去中心化、更高性能和更多功能之间的矛盾浮现出来。可以简单地归结为“安全”与“便利”之间的权衡：去中心化高度安全，但难以实现性能和功能提供的便利性，或良好的用户体验。

安全与便利实际上是人类在给定技术条件下永恒的权衡。根据实际需求分层权衡是理性的解决方式：对安全性要求较高的需求，用去中心化方式满足；对便利性要求高的需求，用中心化的方式实现；对安全性与便利性均适中的需求，用多中心的方式实现。

自由现金系统已经采用了这种分层共识策略：货币、身份、协议、重要关系、重要数据的哈希发布在主链上，实现高度安全，保障基本自由；用户的重要数据存放在多节点的分布式存储中，提高性能和体验的同时，防范信息垄断；用户不重要的大量日常数据存放在本地或中心化云存储中，获得最佳的用户体验。

目前，自由现金主链存储的数据量较小，大量用户数据和公共数据已经开始使用 Freedrive 多节点分布存储系统。借助于自由协议，这些数据并不依赖于 Freedrive，也可以迁移到其他分布式存储（如 IPFS）或中心化存储系统中。

自由现金将继续秉承分工协作、自由竞争的市场经济方向，吸纳和采用互联网经济与密码经济的各种成果、应用和设施，共建分层跨链的自由开放协作体系，增进人类经济自由。

8 自由共识

密码共识始于中本聪实现点对点电子现金的目的，自由现金也是为了实现这一目标改进了中本聪框架。

货币改进的实践表明，单纯的货币去中心化难以改变信息垄断造成的全球经济碎片化，密码共识能够而且必须在更多方面建立去中心化的全球经济基础设施。

在没有事先计划的情况下，自由现金的实践已经扩展到密码身份、密码关系、开放信誉、自由协议、分布存储等领域，并且会继续延伸到更多领域。

“自由现金”已经不能指代这个共识系统的丰富内容了，为此，我们将其扩展为“自由共识”系统，自由现金指代这个系统中的主要货币。

自由共识是密码共识机制的一个实例。“密码共识”一词充分体现了非对称密码和分布式共识构建的去中心化逻辑框架，不应作为实例的名称而造成混淆。

密码共识的目的跟几乎所有人类重大发明一样，都是为了实现更大的人类自由。为此，我们将密码共识的这个实例命名为“自由共识”——自由演进的密码共识系统。