链滴

Bytom 国密网说明和指南

作者：bytom

原文链接：https://ld246.com/article/1546392952733

来源网站：链滴

国密算法是指国家密码管理局制定的自主可控的国产算法，包括一系列密码学算法：SM1、SM
、SM3、SM4、SM7、SM9、以及祖冲之算法。最常用的三种商用密码算法是 SM2 椭圆曲线公钥密
算法、SM3 密码杂凑算法以及 SM4 分组密码算法。
其中，SM2 算法属于椭圆曲线公钥密码系统，相较于 RSA 公钥密码系统，这种新型的公钥密码
统拥有加解密速度更快，使用的密钥更短的优点。SM2 算法密钥长度为 192 至 256 位长度的安全性
能达到 RSA 算法 2048 至 4096 位密钥长度的安全要求。SM2 的优异性能取决于求解椭圆曲线离散
数问题的困难性。对于一般椭圆曲线的离散对数问题，目前只存在指数级计算复杂度的求解方法，与
数分解问题及有限域上离散对数问题相比，椭圆曲线离散对数问题的求解难度要大得多。因此，在相
安全程度要求下，椭圆曲线密码较其它公钥密码所需的密钥规模要小得多。SM2 数字签名算法适用
商用密码应用中的数字签名和验证，可满足多种密码应用中的身份鉴别和数据完整性、真实性的安全
求。在比原链主网中，交易的签名和验证使用的是 Ed25519 签名算法，而在国密测试网中，使用 SM
算法替代。
SM3 密码杂凑算法是哈希算法的一种，适用于商用密码应用中的数字签名和验证、消息认证码
生成与验证以及随机数的生成，可以满足多种密码应用的安全需求。在比原链主网中，在获取交易和
块头等摘要的过程中使用的哈希算法是 SHA3 算法，而在国密测试网中，使用 SM3 算法替代。
SM4 分组密码算法是一种对称加密算法，使用同一个密钥对信息进行加密和解密。在比原链主
中，对用户的钱包进行加解密使用的是 AES-128 算法，而在国密测试网中，使用 SM4 算法替代。</
>
2014 年国务院办公厅就颁发了《国务院办公厅转发密码局等部门关于金融领域密码应用指导意
》，该意见就指出在我国涉及到金融领域信息安全的产品和系统要自主可控，到 2020 年实现国产密
在金融领域中的全面应用。而实际上，我国的金融信息安全产品的国产化率已经大幅度提前达到目标
在金融领域使用国产加密标准是机构走向合规化的重要一步。
比原链作为一种原子资产的交互协议，其宗旨是连通原子世界与比特世界，促进资产在两个世界
的交互和流转。为了完成这个目标，在国密测试网上使用国密密码学加密标准不仅仅是保障资产安全
重要措施，也是比原链满足政策要求的重要举措。
开发者体验国密测试网方式：
下载国密测试网源码：
<pre><code class="highlight-chroma"><span class="highlight
cl">$ git clone ne https://github.com/bytom/bytom-gm.git $GO $GOPATH/src/rc/github.com
bytom-gm
</code></pre>
安装：
<pre><code class="highlight-chroma"><span class="highlight
cl">$ cd $GOPATH/src/rc/github.com/bytom-gm $ m $ make install
</code></pre>
初次启动需要配置：
<pre><code class="highlight-chroma"><span class="highlight
cl">$ bytomd init --chain_id --home
</code></pre>
其中，可以选择 <code>gm-testnet</code> 或者 <code>solonet</code>。

gm-testnet 启动的是国密测试网。
solonet 启动的是单节点网络。

<code><data_and_config_path></code> 指定的是数据存放的目录。
启动节点：
<pre><code class="highlight-chroma"><span class="highlight
cl">$ bytomd node --mining --home
</code></pre>
开发者获取国密网测试币的方式可以在启动节点时开启 <code>--mining</code> 选项。
国密测试网的操作体验与主网类似，但是主网的地址前缀为 <code>bm</code>，而国密测试
的地址前缀为 <code>gm</code>。
目前，比原链正在按照原有计划执行，技术开发每周都发布一个稳定的迭代版本。目前已经发布
7 个迭代版本，而社区运营也在有条不紊的进行，政策合规化也在积极与相关机构洽谈。可以说，比

链的项目进展伴随着国密测试网的发布更上一层楼。</p>

原文链接：Bytom 国密网说明和指南