

技术评测

本期项目：ByteCoin

项目版本：V3.0.0—V3.3.2

1 项目介绍

1.1 说明

本文是对 ByteCoin 进行一个技术评测，所以在评测中有一些关于背景和市场相关的资料借鉴了一些已经公开的文献，如发现雷同纯属正常。文章内容主要是分几个方面对 ByteCoin 从技术到市场等有一个总结分析，然后最后会有一个总结性结论。

字节币，英文全称 Bytecoin，代币简称 BCN，是第一个基于 CryptoNote 技术且致力于匿名反机枪池的、超前的一种货币，2012 年 7 月就已经发布，门罗币就是由字节币分叉而来。Bytecoin 主要是想解决比特币转账的匿名性问题，旨在提供私密、不可追踪的加密货币和个人隐私的清晰解决方案。

1.2 团队成员概况

Bytecoin 社区负责人 Jenny Goldberg 公开介绍，团队目前有四个全职的 C++ 程序员，若干个专职于其他邻域的程序员，一个密码学专家和一个社区管理员。

不过从实际项目的发展情况来看，很可能存在管理不够高效或者实际投入人员并不多得情况，具体请看后面的技术情况环节的介绍。

1.3 市场认知

主要从当前市场的主流相关媒体社区情况来分析总结，截止 2018 年 11 月 2 日：

百度贴吧：没有与 Bytecoin 项目相关的话题讨论。

知乎：Bytecoin 项目相关的话题讨论较少，而话题中提到的也是 18 年 5 月 8 日上线币安的疑似拉高事件。

Facebook：未查询到官方 Facebook 信息。

Reddit：关注者 13.7K。

Twitter：关注量 4.63 万，发布推文及回复数为 2614，评论转发点赞数量较少，基本无粉丝互动，活跃度差。

QQ 社群：近 1500 人，人数较少，活跃度低，广告较多。

Telegram: 中文电报群 545 人，英文电报群 12952 人，未发现大量僵尸粉，但粉丝人数较少，活跃度不高。

2012 年发布至今，其市场地位与门罗币等，远远不及。中国市场目前由 Joey Ji（冀纯强）负责，主要是组织建设字节币的中国区社群。

1.4 市值说明

截至 2018 年 11 月 1 日：

字节币 BCN 代币市值 **237,325,379** 美元，每一个代币合美元 0.0012893436，合 RMB 为 0.008766338。

1.5 交易所

截止 2018 年 11 月 2 日：

字节币 BCN 目前已上线交易所 8 家，近几日二级市场 24h 成交额 **\$326,258**。

1.6 市场风险

字节币的应用场景跟知名币如以太坊等相比，其场景比较单一，由于其他匿名特性，主要用于支付市场。而不能支持其他如 Dapp 等业务场景。

价格操纵风险：字节币发行量庞大，80%的币在 2014 年之前就已经被挖出来，存在团队预挖的可能。预挖可能导致 Bytecoin 的大量筹码集中在少数人手里，容易对价格实施操纵。所以该项目现在的新用户基本很难有强烈的加入感。

恶意拉盘风险：今年 5 月上线币安时，BCN 成交价不断上升，疯狂拉涨 32 倍，而后价格迅速回落，疑似是该团队锁定了全网钱包转账，制造大量的虚假交易量，涉嫌恶意拉盘。

1.7 发展前景

就目前来看，字节币的发行量、价格定位，在小额支付行业会有较大的需求；而且其本身的加密特性，在一些“颜色领域”等，也会有比较强的需求。

2 功能评测

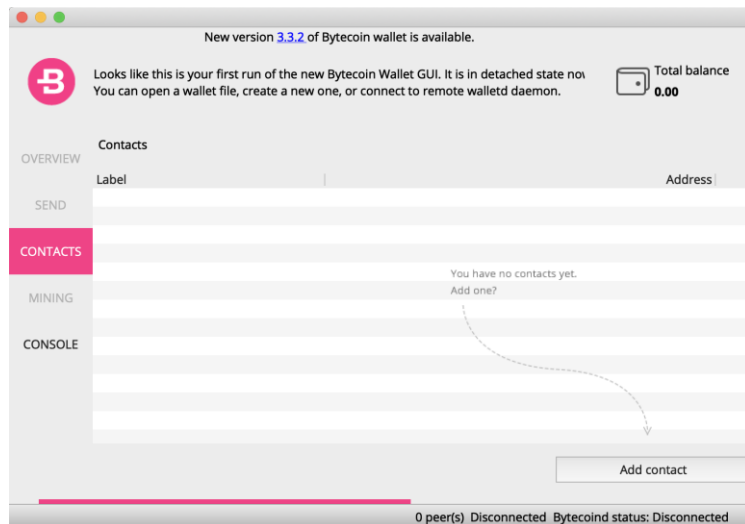
对比白皮书描述功能和已经实现功能之间功能本身与性能之间的差异（具体：区块浏览器、钱包和主程序运行测试区块链基本功能和实现度，通过统计数据测试性能）

- 区块浏览器：

地址：<https://bytecoin.money/>，只有最精简的功能：创建地址，买币。没有其它任何功能，对于这样长时间的项目来说，非常的不正常。也许存在人员不足的问题？

- 钱包：

MAC 版本下载安装之后，一直在连服务器，无法成功连接。采用 VPN 的方式，排除网络防火墙影响情况下，仍然是无法打开，不清楚是不是其服务器已经停止运作，还是有其它 BUG 问题：



- 移动端，只有 Android 版本
- 主程序安装部署测试

需要安装的 C 环境依赖比较多，在 Ubuntu16 上部署测试还算比较顺利。

使用情况：

在没有提交交易的情况下，自动出块高度到 249976 时，进程崩掉，原因是一个 double free or corruption。目前它的开源版本只能说是能跑起来，一旦稍微运行时间久了以后就会直接奔溃，处于不可用的 Beta 阶段。重启之后尝试恢复，依旧报日志无法写入的错误。主程序表面上结果是运行不稳定，如下

图：

```
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
15:58:45.317852 I P2P Connecting to=76.169.236.235:8080
Received block with height=209004 (queue=1) from 144.217.84.27:8080
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
15:58:51.509053 I BlockchainState redo_block height=209004 bid=df910426af1c0783ac7f6455acfe7ee
fd335f6e9bafbed131fe55a45c6ae64ad #tx=0
Received block with height=209464 (queue=0) from 144.217.84.27:8080
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
15:58:58.379196 I BlockchainState redo_block height=209464 bid=fa7e11f7aabc639783eecd0db3d95ebb
10b0fbb4b88fbf9e70dffa87e0ef9390e #tx=0
Log File Write Failed, error=Error writing file, errno=28
15:58:58.530412 I Node Added last (from batch) downloaded block height=209998 bid=8ff32e749a13
500f0b4506d9a8090beb43f70daac0ef70beed0dce2053f08fb3
Log File Write Failed, error=Error writing file, errno=28
15:58:58.532443 I Node DownloaderV11::advance_chain Requesting chain from 144.217.84.27:8080 r
emote height=1633143 our height=209998
Log File Write Failed, error=Error writing file, errno=28
15:59:06.407315 I P2P Connecting to=67.246.74.32:8080
P2p COMMAND_HANDSHAKE response version=1 unique_number=1498504611007272400 current_height=164
5428 local_peerlist.size=252 from 67.246.74.32:8080
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
Log File Write Failed, error=Error writing file, errno=28
```

```

/libcrypto.so.1.0.0
7fbd0f2e5000-7fbd0f301000 r--p 00219000 08:01 656362 /lib/x86_64-linux-gnu
/libcrypto.so.1.0.0
7fbd0f301000-7fbd0f30d000 rw-p 00235000 08:01 656362 /lib/x86_64-linux-gnu
/libcrypto.so.1.0.0
7fbd0f30d000-7fbd0f310000 rw-p 00000000 00:00 0
7fbd0f310000-7fbd0f36e000 r-xp 00000000 08:01 656368 /lib/x86_64-linux-gnu
/libssl.so.1.0.0
7fbd0f36e000-7fbd0f56e000 ---p 0005e000 08:01 656368 /lib/x86_64-linux-gnu
/libssl.so.1.0.0
7fbd0f56e000-7fbd0f572000 r--p 0005e000 08:01 656368 /lib/x86_64-linux-gnu
/libssl.so.1.0.0
7fbd0f572000-7fbd0f579000 rw-p 00062000 08:01 656368 /lib/x86_64-linux-gnu
/libssl.so.1.0.0
7fbd0f579000-7fbd0f59f000 r-xp 00000000 08:01 661999 /lib/x86_64-linux-gnu
/ld-2.23.so
7fbd0f61a000-7fbd0f786000 rw-p 00000000 00:00 0
7fbd0f799000-7fbd0f79a000 rw-p 00000000 00:00 0
7fbd0f79a000-7fbd0f79c000 rw-s 00000000 08:01 397950 /home/jingqingyun/.by
tecoin/peer_db/lock.mdb
7fbd0f79c000-7fbd0f79e000 rw-s 00000000 08:01 395911 /home/jingqingyun/.by
tecoin/blockchain/lock.mdb
7fbd0f79e000-7fbd0f79f000 r--p 00025000 08:01 661999 /lib/x86_64-linux-gnu
/ld-2.23.so
7fbd0f79f000-7fbd0f7a0000 rw-p 00026000 08:01 661999 /lib/x86_64-linux-gnu
/ld-2.23.so
7fbd0f7a0000-7fbd0f7a1000 rw-p 00000000 00:00 0
7ffc07d77000-7ffc07d99000 rw-p 00000000 00:00 0 [stack]
7ffc07df1000-7ffc07df4000 r--p 00000000 00:00 0 [vvar]
7ffc07df4000-7ffc07df6000 r-xp 00000000 00:00 0 [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0 [vsyscall]
已放弃 (核心已转储)

```

跟现在主流链相关的项目使用容器 Docker 来部署明显运维不熟技术成就，还是采用自动脚本不熟，环节依赖还是较多，项目部署的上线方式还是几年前比较陈旧的方式。

3 代码质量

1. Github 的项目相关源码使用 C++语言实现，除了相关 API 文件添加了一些注释，其余具体功能实现代码部分基本没有注释，造成阅读源码很困难，而且无相关技术文档，通过官网查询相关文档，有的文档网页无法打开。该项目基本工程化比较差，基本无可维护性。
2. 源代码中包括了日志处理模块、P2P 传输模块、加密算法模块(包含 POW)、钱包等模块，能够完整的实现一个区块链功能，包括节点之间的信息传输、区块链中链的数据结构等等，代码中都有体现，作为一个链的基本功能模块已经齐备。
3. 该项目主要创新算法采用的是 CryptoNote，该算法是一个开源项目，github 上也有该项目，源码都是公开。该技术主要有如下几大特点：环签名实现匿名支付，交易无法追踪、更加公平的 POW 算法、智能调整区块链参

数。目前基于该技术的数字货币除了 BCN 外，还有门罗币、AEON、BBR、FCN 等。通过查看源码，基本直接套用的 CryptoNote，所以其算法是具有可现实度的。

通过查阅起官网、社区等社交媒体，目前没有查询到其锁仓计划相关资料，而且该项目目前也没有发现有智能合约相关功能。

4. 代码质量工具分析

借助业界常用的静态代码分析工具，对 Bytecoin 代码的 src 目录和 tests 目录，进行静态分析。其结果很不理想，理论上 error 的问题一般是必须要解决，如果一个项目能有上千的 error，其团队的开发工程化能力非常的堪忧，所以前面测试的直接崩溃现象也是可以理解的了。统计结果如下：

src 目录代码文件 104 个，发现 error: 2366

tests 目录代码文件 8 个，发现 error: 10 个，warn 383 个

```
20/104 files checked 20% done
Checking src/CryptoNote.hpp...
<error file="src/CryptoNote.hpp" line="43" id="unusedStructMember" severity="style" msg="struct member &apos;CoinbaseInput::height&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="61" id="unusedStructMember" severity="style" msg="struct member &apos;TransactionOutput::amount&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="84" id="unusedStructMember" severity="style" msg="struct member &apos;ParentBlock::major_version&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="85" id="unusedStructMember" severity="style" msg="struct member &apos;ParentBlock::minor_version&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="86" id="unusedStructMember" severity="style" msg="struct member &apos;ParentBlock::timestamp&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="88" id="unusedStructMember" severity="style" msg="struct member &apos;ParentBlock::nonce&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="89" id="unusedStructMember" severity="style" msg="struct member &apos;ParentBlock::transaction_count&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="111" id="unusedStructMember" severity="style" msg="struct member &apos;BlockBodyProxy::transaction_count&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="131" id="unusedStructMember" severity="style" msg="struct member &apos;SendProof::amount&apos; is never used."/>
<error file="src/CryptoNote.hpp" line="161" id="unusedStructMember" severity="style" msg="struct member &apos;SWCheckpoint::height&apos; is never used."/>
35/104 files checked 34% done
49/104 files checked 48% done
Checking src/Core/WalletSerializationV1.cpp...
<error file="src/Core/WalletSerializationV1.cpp" line="28" id="unusedStructMember" severity="style" msg="struct member &apos;ObsoleteSpentOutputDto::amount&apos; is never used."/>
<error file="src/Core/WalletSerializationV1.cpp" line="30" id="unusedStructMember" severity="style" msg="struct member &apos;ObsoleteSpentOutputDto::output_in_transaction&apos; is never used."/>
<error file="src/Core/WalletSerializationV1.cpp" line="31" id="unusedStructMember" severity="style" msg="struct member &apos;ObsoleteSpentOutputDto::wallet_index&apos; is never used."/>
<error file="src/Core/WalletSerializationV1.cpp" line="38" id="unusedStructMember" severity="style" msg="struct member &apos;ObsoleteChangeDto::amount&apos; is never used."/>
<error file="src/Core/WalletSerializationV1.cpp" line="43" id="unusedStructMember" severity="style" msg="struct member &apos;UnlockTransactionJobDto::block_height&apos; is never used."/>
<error file="src/Core/WalletSerializationV1.cpp" line="45" id="unusedStructMember" severity="style" msg="struct member &apos;UnlockTransactionJobDto::wallet_index&apos; is never used."/>
28/104 files checked 15% done
```

注意：由于检查软件自身缺陷和规则限制可能会有漏侧和误报现象。

2. 详细扫描结果请查看下面的 xml 文件



result-1.xml



result-2.xml

4 技术能力

- 白皮书中对于技术逻辑的论证以及推到是否真实可信。

依托于 **CryptoNote**，所以最主要的隐藏属性不会有实现的问题，其它功能和常规的链没有大的区别，所以起方案技术逻辑是可信的。

- 抄袭情况，区块链项目都为开源，思路借鉴在所难免，主要看是否有直接的抄袭。

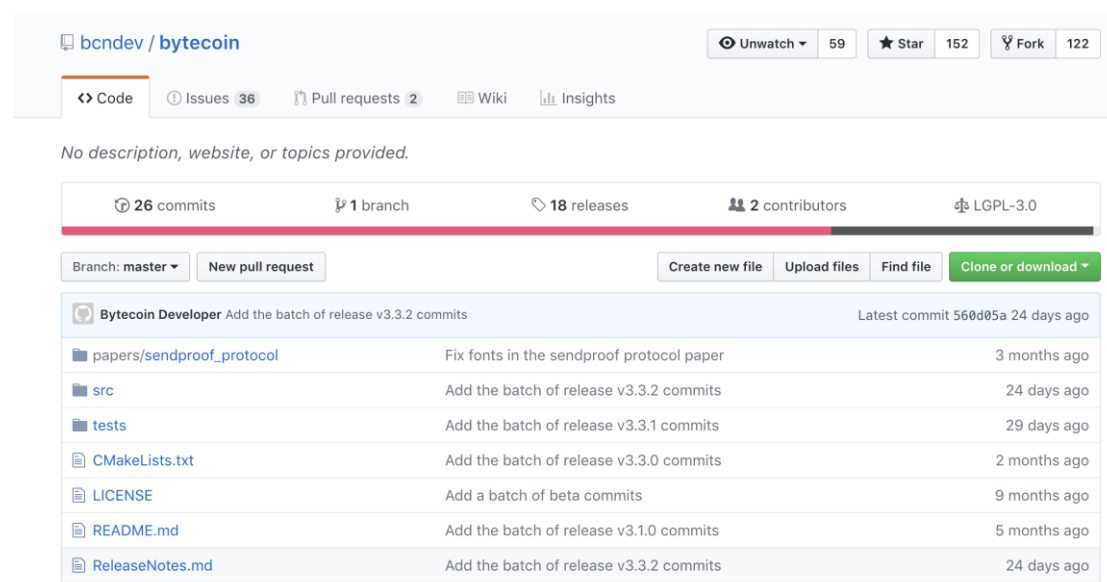
虽然主要功能直接使用了 **CryptoNote** 来实现，包括中间也有一些其它的 P2P 的开源组件，但是都尊重了开源协议信息了公开，所以没有问题。

- 代码的社区情况，比如贡献者参与度、代码的更新频率、代码的查看与评论频率。

项目 bcndev/bytecoin，从版本 3.0 开始，做过迁移，目前地址为：

<https://github.com/bcndev/bytecoin>

分支只有一个 Master 分支，Star 数量为 152，Fork 数量 122。



bcndev / bytecoin

Unwatch 59 Star 152 Fork 122

Code Issues 36 Pull requests 2 Wiki Insights

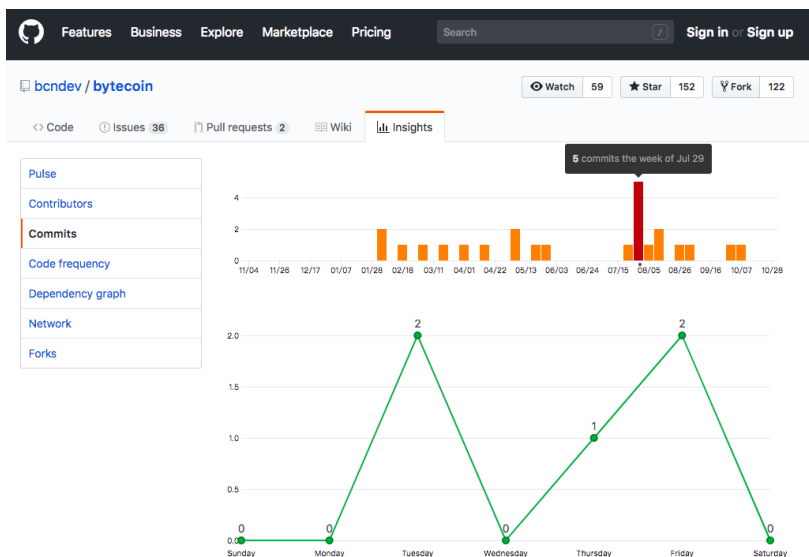
No description, website, or topics provided.

26 commits 1 branch 18 releases 2 contributors LGPL-3.0

Branch: master New pull request Create new file Upload files Find file Clone or download

Commit	Message	Time
Bytecoin Developer	Add the batch of release v3.3.2 commits	Latest commit 560d05a 24 days ago
papers/sendproof_protocol	Fix fonts in the sendproof protocol paper	3 months ago
src	Add the batch of release v3.3.2 commits	24 days ago
tests	Add the batch of release v3.3.1 commits	29 days ago
CMakeLists.txt	Add the batch of release v3.3.0 commits	2 months ago
LICENSE	Add a batch of beta commits	9 months ago
README.md	Add the batch of release v3.1.0 commits	5 months ago
ReleaseNotes.md	Add the batch of release v3.3.2 commits	24 days ago

Master 分支平均每个月，有 3 次左右的大版本的提交。

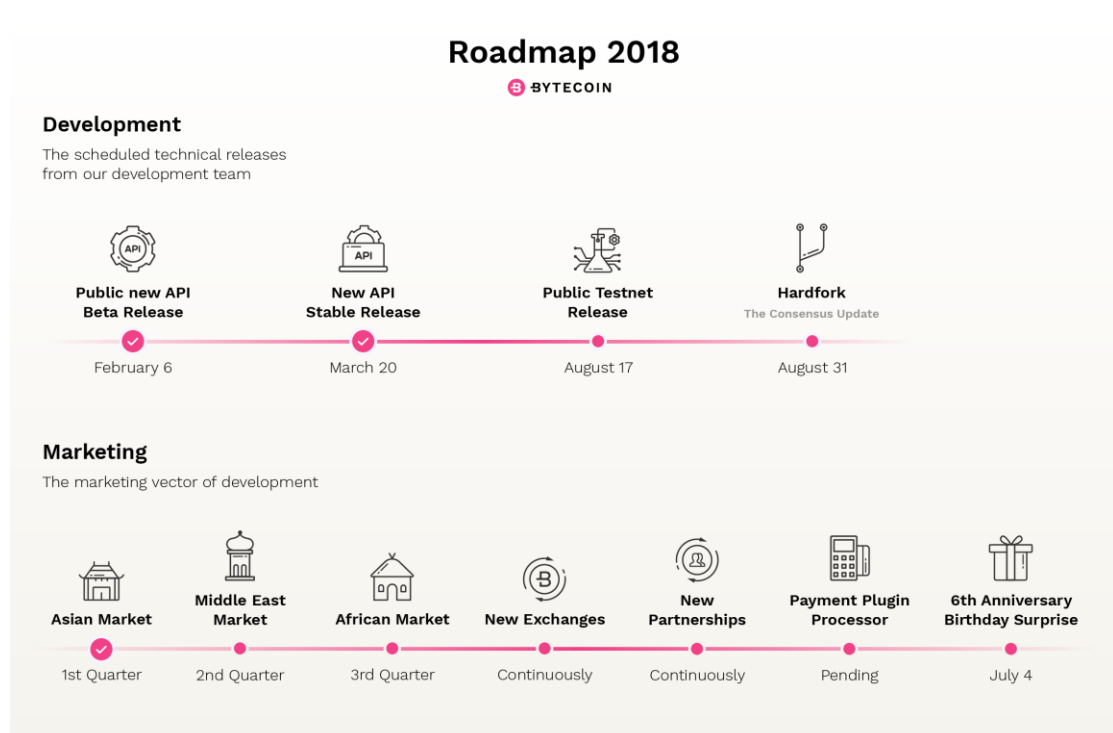


- 结合代码本身判断是否和真正的程序吻合，是否出现代码实现与发布的程序不吻合的情况。

代码为 C++，项目实际时间比较长，初步看来，未发现特别明显的问题。只是代码质量不够好。

5 产品推进计划

2018 年最新 Roadmap



开发路线：

1. 通过 github 可以看到，2 月 6 日和 2 月 19 提交了两个 beta 版本，通过 commit 可以发现，主要修改了一些头文件的引用、代码实现以及代码格式，代码功能的完成度较高。
2. 原计划 3 月 20 日发布的 release 版，在 git 上 3 月 22 日发布了正式 release 版。
3. 计划 8 月 17 号上线的测试网络，18 号上线，下载相关的客户端并运行，可以加入测试网络网络，并且能够实现交易、挖矿等功能。通过日志可以看到节点之间请求和返回数据。
4. 硬分叉 github 上，在 8 月 31 号发布了 v3.3.0 版本，该版本更新了 API、consensus、命令等，并设定了硬分叉条件，当 24 小时内新版本的块达到 90%就自动完成切换，最终于 2018 年 10 月 1 号下午 7 点 11，区块高度 1629055 完成硬分叉。

总结，按照 roadmap，查看相关的源代码，相对比较准时，最多晚一两天，代码完成度的功能也实现，只是从前面的实际代码质量分析来看，代码质量不够好。

市场路线：

1. 目前已开通印度、俄罗斯、土耳其、意大利、西班牙社区。
2. 15 家数字交易所支持 BCN 交易。[Poloniex](#)、[HitBTC](#)、[Bytecoin Web Wallet](#)、[Coinspot](#)、[Cryptonator](#)、[Changelly](#)、[Stocks.exchange](#)、[Best Rate](#)、[Godex](#)、[Vebitcoin](#)、[TradeOgre](#)、[Cfinex](#)、[Crex24](#)、[Gate.io](#)、[Bitexbook.com](#)

6 总结:

ByteCoin 作为一个历史悠久的项目，从功能完成度上的确做到了基本按照白皮书规划的功能项来进行。但是其核心功能代码全部借鉴 [CryptoNote 的代码](#)，所以该项目的技术核心的突破前进，受限于 CryptoNote 的发展。同时所有对应的功能按计划在完成，但是从实际代码质量来看比较糟糕，也缺乏代码的工程化可维护性。很多作为产品的细节，基本上都按照最简功能来实现，而且很粗糙，甚至出现无法直接使用和服务无法连接崩溃的现象，和同类产品无法竞争。在运营方面也出现疑似操作价格的情况，同时在设计上没有充分得考虑价值稀缺性的加强设计，到现在百分之 80 的价值资源基本都已经挖掘完备，缺乏新的动力，整个活跃度和热度也相应较低。