

BSC 测试网 外部测试指南

安全接入、钱包准备、真实交易测试、证据反馈与故障排查

适用对象	经 Pravelle 运营方批准的封闭测试人员
测试网络	BNB Smart Chain Testnet Chain ID 97 tBNB
测试入口	https://pravelle.vercel.app/app.html?network=testnet
配套隧道	pravelle-tester-tunnel v1.0.1
版本	1.2 2026-07-23

1. 先读这一页：安全边界

最高优先级：只使用专用测试钱包、tBNB、pTST 和 pUSD。不要连接持有主网资产的钱包。不得向任何人发送助记词、钱包私钥、恢复文件、恢复口令、SSH 私钥或 prover token。

本指南用于受控、限时开放的 BSC Testnet 窗口。DarkPool 在窗口外由 2-of-3 Safe 多签暂停。即使网页仍可打开，只有在运营方明确发出“窗口已开放”通知后才能提交链上交易。

隐私边界必须准确理解：池内票据所有权和订单承诺被隐藏；充值时的代币与金额、提现时的代币、金额与收款地址仍会公开上链。Matcher 会看到订单方向、价格、数量、交易对和到期时间，因此不要使用真实交易意图。

任何一项出现时立即停止

- 钱包显示 BSC 主网或任何非 97 的 Chain ID。
- SSH 指纹与运营方交接值不完全一致，或 SSH 意外打开远程 shell。
- 网页域名不是 `pravelle.vercel.app`，HTTPS 证书异常，或 DarkPool 地址不同。
- prover、matcher、索引器、ASP、Safe 状态或链上 root 出现不一致。
- 运营方发出“窗口关闭”或紧急停止通知。

建议顺序

阶段	内容	是否上链
0	阅读交接表、Demo、端口与软件准备	否
1	SSH 指纹、隧道、token 和 health 检查	否
2	连接钱包、创建账户、下载恢复文件	仅免费签名
3-6	充值、下单、取消、提现、指定人员 half-match	是
7	负向测试、反馈、清理与凭据吊销	通常否

2. 本批次交接表

运营方必须通过批准的私密渠道把下表完整交给每位测试者。任何空项都应在测试前补齐；公开 PDF 不包含真实主机、token 或内部联系方式。

字段	运营方填写
批次 / 测试者 ID	_____
允许的测试项与 half-match 角色	_____
窗口开始 / 结束 / 时区	_____
应用 URL 与预期部署版本	_____
SSH 别名、HostName、User、Port	_____
网关 / 最终主机 SHA256 指纹	_____
SSH 公钥启用 / 吊销时间	_____
prover token 到期 / 轮换时间	_____
tBNB / pTST / pUSD 发放量	_____
half-match 对手方与协调频道	_____
私密支持 / 安全上报渠道	_____
紧急停止通知的准确格式	_____

推荐软件基线：最新版 Chrome + MetaMask，使用干净浏览器 Profile，并禁用其他注入式 EVM 钱包扩展。Phantom、Trust Wallet、Keplr 等其他钱包仅作为 best-effort 测试。

操作系统：公开隧道支持 macOS 和 Linux。原生 Windows 未验证；除非运营方提供已验证的 WSL2 流程，否则请使用受支持设备。

3. 钱包、网络与测试资产

- 新建专用测试钱包，钱包内没有任何主网资产。
- 网络显示 BNB Smart Chain Testnet，Chain ID 为 97。
- 钱包有运营方指定数量的 tBNB、pTST 和 pUSD。
- 浏览器只有一个启用的 EVM 钱包扩展。
- 运营方已确认测试窗口和分工。

网络字段	准确值
网络名称	BNB Smart Chain Testnet
RPC URL	https://bsc-testnet-dataseed.bnbchain.org
Chain ID	97
货币符号	tBNB
区块浏览器	https://testnet.bscscan.com

合约 / 代币	地址
DarkPool	0xBE945fADB5917FdD20f7cA46A76163b17B526E0f
Verifier	0xE518b138b5AC298993c470102F06b21d5419238d
pTST	0x6f8807E70c7DE2d218388Fb2D9418190A48481C9
pUSD	0x42003a22247B271caeA327944a62aA5Ce46989D7

pTST 与 pUSD 均为 18 decimals。Guided 模式输入整数 base units，且不得超过 9007199254740991。建议小额为 10000000000000000 base units，即 0.001 token，最终以交接表为准。

tBNB 获取： 优先由运营方直接向专用测试钱包发放。不要为了满足网页水龙头条件而向该钱包转入主网 BNB。需要水龙头时，只使用运营方确认的 BNB Chain 官方文档所列 Discord、Telegram 或其他批准渠道。

4. 生成 SSH 密钥并核对主机指纹

4.1 测试者在本机生成专用密钥

```
ssh-keygen -t ed25519 -a 64 \  
-f ~/.ssh/pravelle-tester \  
-C "pravelle-bsc-testnet"  
chmod 600 ~/.ssh/pravelle-tester
```

设置强口令。只把 `~/.ssh/pravelle-tester.pub` 发给运营方。没有 `.pub` 后缀的是私钥，必须留在本机，运营方也不需要知道它的本地路径。

4.2 运营方返回的内容

- 准确的 SSH alias 配置：Host、HostName、User、可选 Port。
- 网关和最终主机的 SHA256 指纹，通过独立认证渠道发送。
- 密钥启用与吊销时间。

4.3 首次连接前核对

```
ssh-keyscan -t ed25519 运营方提供的真实主机名 \  
> /tmp/pravelle-host-key  
ssh-keygen -lf /tmp/pravelle-host-key
```

非 22 端口时给 `ssh-keyscan` 增加 `-p` 端口号。显示的 `SHA256:...` 必须与交接表逐字一致。完全一致后才安装：

```
mkdir -p ~/.ssh && chmod 700 ~/.ssh  
ssh-keygen -H -f /tmp/pravelle-host-key  
grep -v '^#' /tmp/pravelle-host-key >> ~/.ssh/known_hosts  
chmod 600 ~/.ssh/known_hosts
```

指纹不一致、未知或发生变化时，不要输入 `yes`，不要删除 `known_hosts` 绕过检查。停止并通过私密支持渠道联系运营方。使用 ProxyJump 时，网关和最终主机都要独立核对。

5. 下载、验证并启动公开隧道

公开仓库：<https://github.com/cysic-labs/pravelle-tester-tunnel>

发布版本：**v1.0.1**；压缩包 SHA256：

```
4346c66d82f156a7d366e7f8edee5593a823db2695d922ca1763817f7bbcdc86
```

```
TUNNEL_VERSION=v1.0.1
BASE="https://github.com/cysic-labs/pravelle-tester-tunnel/releases/download/$TUNNEL_VERSION"
curl -fLO "$BASE/pravelle-tester-tunnel-$TUNNEL_VERSION.tar.gz"
curl -fLO "$BASE/SUMS"

# macOS; Linux 使用 sha256sum -c SUMS
shasum -a 256 -c SUMS
tar -xzf "pravelle-tester-tunnel-$TUNNEL_VERSION.tar.gz"
cd "pravelle-tester-tunnel-$TUNNEL_VERSION"
shasum -a 256 -c SUMS
./tests/test.sh
```

两个 checksum 检查和离线测试都必须成功。随后确认端口空闲：

```
# macOS
lsof -nP -iTCP:8798 -sTCP:LISTEN
lsof -nP -iTCP:8799 -sTCP:LISTEN

# Linux
ss -ltn '( sport = :8798 or sport = :8799 )'
```

无输出表示空闲。不要结束不认识的进程；端口已占用时联系运营方。启动：

```
./bin/pravelle-tester-tunnel \
运营方提供的受限别名 ~/.ssh/pravelle-tester
```

保持终端运行。v1.0.1 会拒绝未知或变化的 SSH 主机密钥，只建立本机 127.0.0.1:8798 与 :8799 转发。若出现远程 shell，立即退出并上报。

6. 浏览器、token 与账户恢复

6.1 检查本地服务

```
curl -fsS http://127.0.0.1:8798/health
curl -fsS http://127.0.0.1:8799/health
```

Matcher 应返回 `{"ok":true}` ; prover 应显示 `ok`、`proverReady:true` 和 `authConfigured:true`。浏览器与隧道必须在同一台机器上。

6.2 设置短期 prover token 与 ASP

只打开 <https://pravelle.vercel.app/app.html?network=testnet>。在浏览器 Console 运行：

```
localStorage.setItem(
  "pravelle:proverToken",
  prompt("Paste the test-window prover token")
);
localStorage.removeItem("pravelle:aspUrl");
location.reload();
```

不要截图 token、Console、localStorage 或带认证头的网络请求。新版 Guided 页面会自动检查 active ASP：新充值先显示“Awaiting association approval”，operator 批量更新 root 后会自动变成“Association approved”并解锁下单，不需要 tester 填 commitment 或 root。

6.3 创建私有账户

1. 选择 Guided，连接专用 MetaMask 钱包并确认 Chain ID 97。
2. 批准一次免费账户解锁签名。它不是链上交易。
3. 创建独立恢复口令，立即下载加密 recovery JSON。
4. 将 recovery JSON 与恢复口令分开保存。
5. 资金进入前完成一次恢复演练：重新打开页面，选择 Import recovery。

账户地址、钱包地址、Chain ID、DarkPool 地址或恢复文件所属网络不一致时停止。不得修改 JSON 绕过检查。

7. Demo 与真实充值

7.1 Walletless Demo

步骤	操作	通过标准
A1	Try demo without wallet	明确显示 sample only，不触发钱包签名
A2	Add sample funds	样例余额与 Activity 更新，不上链
A3	Place / Withdraw sample	不出现钱包确认，Demo 与真实账户隔离

7.2 真实充值

1. Guided 中点击 Add funds，填写交接表指定的 pTST 或 pUSD 完整地址。
2. 输入小额整数 base units，不得超过 9007199254740991。
3. 等待 preparing、submitting、proving、wrapping。通常 45-90 秒，排队时更久；不要重复点击。
4. 如需 approve，核对 spender 必须为 DarkPool 0x8A94...8Ed6，批准金额不要高于测试所需。
5. 证明完成后确认 deposit，等待 BscScan status = Success。
6. Activity、私有余额、新 note 与链上 receipt 必须一致。

检查项	通过标准
Prover	生成 job 并最终返回 proof；无 master-key 字段错误
Approve	spender 和金额正确，status = 1
Deposit	目标合约、Chain ID、金额正确，status = Success
Indexer	新 note 可发现，chain sync 无 root mismatch

8. 下单、取消与提现

8.1 隐藏订单

1. 选择交接表规定的 side、price、size、base、quote 和 expiry。
2. 核对 base / quote 完整地址，不使用真实交易意图。
3. Place order 后等待真实 Venus proof；proof 的时间窗口有限，过期必须重建。
4. 确认钱包目标为 DarkPool，receipt 成功后 Activity 应出现订单记录。

8.2 取消订单

1. 只取消本批次、当前账户创建的订单。
2. 等待 cancel proof，不要在队列中重复点击。
3. 确认链上 receipt 成功，订单状态变为 cancelled，相关 nullifier 不可重复使用。

8.3 小额提现

1. 先确认 ASP readiness、association root、blocklist root 和 chain sync 正常。
2. 选择本批次 note，输入交接表指定的小额和测试钱包收款地址。
3. 等待 transfer proof；通常约 90-150 秒，排队时更久。
4. 钱包确认前核对 token、amount、recipient、DarkPool 和 Chain ID 97。
5. receipt 成功后，公开收款余额增加，私有余额减少，旧 note 不可再次花费。

隐私说明：提现的 token、amount 和 recipient 是公开链上数据；隐藏的是所花费私有 note 的链接关系。不要把“提现完全隐藏”作为通过标准。

9. 指定人员：half-match 结算

只有交接表明确指定的两名技术测试者可以执行。双方必须在同一窗口、同一交易对和协调频道内操作；其他测试者跳过本页。

参与者 A

- 确认指定 side、price、size、base、quote。
- 生成自己的 half-match proof。
- 只共享 matcher 要求的公开 linkage 和 proof 结果。
- 不共享 recovery、spending key 或 master key。

参与者 B

- 独立核对相反 side 和相同交易参数。
- 生成自己的 half-match proof。
- 确认联合状态与预期完全一致。
- 不接收或要求 A 的任何私密密钥材料。

提交者检查

1. 两个 proof 均成功，joint ID、订单承诺、token 对、price、size、expiry 一致。
2. settleMatch2 的目标是当前 DarkPool，Chain ID 97，gas 估算未超过协议上限。
3. 只有交接表指定的提交者广播。
4. receipt status = Success 后，双方 Activity、余额、输出 notes 和订单状态一致。
5. 保存交易哈希与双方各自的脱敏 job ID，不保存 token 或私密 witness。

停止条件

- 任一 proof 过期、参数不一致、根不一致、订单已取消或 matcher 会话变化。
- 任何一方要求通过聊天发送私钥、recovery 文件或 token。
- 运营方未准备可立即执行的重新暂停交易。

10. 负向测试与故障排查

测试	预期结果
错误 Chain ID	页面阻止继续，不提交证明或交易
错误 / 缺失 prover token	返回认证错误，不泄露内部信息
8798 / 8799 未启动	health 失败，界面给出明确提示
未知 SSH 主机密钥	v1.0.1 客户端拒绝连接
金额超过安全整数	客户端拒绝输入
错误 token / DarkPool 地址	核对失败并停止
重复点击或旧 proof	不产生不可解释的重复状态；过期 proof 被拒绝

排查顺序

1. 确认窗口仍开放、应用域名正确、Chain ID = 97。
2. 确认只有一个 EVM 钱包扩展启用，刷新后重新连接。
3. 检查隧道终端是否仍运行，再检查两个 health URL。
4. 确认 token 未过期、ASP URL 正确、chain sync 无 root mismatch。
5. 查看脱敏后的浏览器错误、job ID、交易哈希和 BscScan receipt。
6. 仍无法确认时停止，不要反复广播，并联系私密支持渠道。

Address already in use：先用第 6 页的命令找出监听进程。不要使用 `kill -9` 或结束不认识的系统服务；把脱敏进程名和端口报告给运营方。

SSH WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED：不要删除 `known_hosts` 继续连接。停止并要求运营方重新确认基础设施与指纹。

11. 反馈、证据与测试结束

11.1 脱敏反馈模板

```
批次 / 测试者 ID:  
时间与时区:  
操作系统 / Chrome / MetaMask 版本:  
测试用例:  
预期结果:  
实际结果:  
Chain ID:  
应用部署版本:  
隧道版本: v1.0.1  
脱敏 job ID:  
交易哈希 / BscScan URL:  
错误原文 (已移除 token、主机、私钥路径):  
是否仍可能继续广播: 否 / 不确定 / 是
```

通过交接表中的私密支持渠道发送。不要在公开 GitHub Issue 中提交实时凭据、真实内部主机、未修复漏洞或指纹异常。

11.2 禁止保存或发送

- 钱包或 SSH 私钥、助记词、recovery 文件、恢复口令。
- prover token、Authorization header、localStorage 截图。
- 完整私密 witness、master key、spending key 或内部主机配置。

11.3 结束清单

- 运营方确认测试窗口关闭，DarkPool 已重新暂停。
- 停止隧道终端并关闭测试浏览器 Profile。
- 清除短期 prover token；保留 ASP 公共 URL 不构成秘密。
- 运营方吊销测试者 SSH 公钥并轮换 prover token。
- 测试者删除不再需要的专用 SSH 私钥，或按运营方保留策略封存。
- 只保留 receipt、交易哈希、脱敏 job ID 和最终报告。

最终通过标准：运营方从独立 RPC 确认 `DarkPool.paused() == true`，所有测试凭据已吊销或轮换，证据不含秘密。

公开参考：BNB Chain wallet configuration、JSON-RPC endpoint 与 faucet 文档；Pravelle Tester Tunnel v1.0.1 release；本 PDF 的稳定地址为 <https://pravelle.vercel.app/pravelle-bsc-testnet-external-testing-guide-zh.pdf>。