

DDC 保管箱用户手册

Version 1.0.1

北京红枣科技

目录

1	扩展应用说明	1
2	安装扩展	2
2.1	Chrome Webstore(需要翻墙)	2
2.2	Microsoft Edge Extensions Home	4
2.3	官方下载压缩包	5
3	使用说明	7
3.1	第一次使用	7
3.2	创建密码	7
3.3	助记词	8
3.4	解锁保管箱	9
3.5	签名	9
3.6	显示私钥	10
3.7	修改账户名和备注	11
3.8	新建账户	11
3.9	导入账户	12
3.10	通过助记词导入	13
3.11	忘记密码	14
3.12	查看 DDC 信息	14

1 扩展应用说明

DDC 保管箱是一个开源的私钥保管工具，旨在帮助用户安全保存、独立管理和便捷使用属于自己的私钥，也为平台开发者们提供了一个能够快速满足自身用户本地管理和使用私钥需求的工具。保管箱并不限于提供基于 DDC 的服务，任何需要通过私钥签名的功能场景均可被集成到保管箱中，例如无密码登录、身份授权等。根据用户需求不同，DDC 保管箱将为以下三类用户提供支持：

- **最终用户：**用户可在保管箱内生成私钥或者将已有私钥导入到 DDC 保管箱扩展应用中，保管箱将私钥安全的存储在用户本地。当遇到需要使用私钥的情况时，用户可通过与保管箱快捷方便的互动完成对于私钥的使用。
- **网站开发者：**通过简单方便的方式快速将保管箱与自身网站业务进行集成，为网站用户提供例如无密码登录、自动唤醒保管箱进行签名等功能来提高用户友好性，避免用户自己保管私钥，却不会使用导致网站被迫需要托管用户私钥，从而造成互信成本大幅提高。
- **进阶开发者：**保管箱的代码将完全开源，对于需求复杂的开发者们可引用开源代码任意搭建属于自己的私钥保管箱，也可以在保管箱定制开发与自己的应用进行集成。我们期待与您的深度交流与合作。

此版本‘DDC 保管箱’扩展应用将支持以下主要功能：

- ✧ 创建账户
- ✧ 导入、导出私钥
- ✧ 私钥签名
- ✧ 官方 DDC 查询

由于各个框架签名机制并不一致，此版本保管箱兼容武汉链、泰安链，后期会尽快兼容其余底层框架。

由于各浏览器扩展应用开发逻辑不同，此版本保管箱兼容 Chrome 浏览器和 Edge 浏览器，后期会尽快兼容其它浏览器。

2 安装扩展

‘DDC 保管箱’已经在 Chrome Webstore 和 Microsoft Edge Extensions Home 上架，用户可前往对应商店进行下载安装。用户也可以从 BSN 官方门户下载相应安装包，通过 Chrome、Edge 浏览器的开发者模式进行扩展安装。三种方式的具体流程如下：

2.1 Chrome Webstore

首先打开 Chrome 浏览器，找到上方工具栏中的扩展管理控件。



点击控件进入 Chrome 扩展程序管理页面，点击 Chrome 网上应用店，跳转至 Chrome 网上商店。

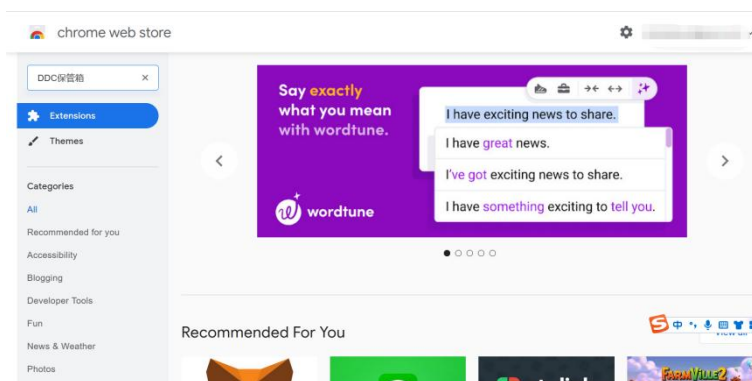


也可通过点击左上方选项栏进行跳转。





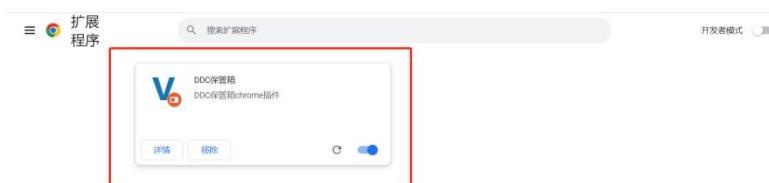
进入 Chrome Webstore 扩展应用商店以后，搜索‘DDC 保管箱’。



找到‘DDC 保管箱’扩展应用后进行下载安装。



安装完成后，在 Chrome 扩展应用管理界面将会出现‘DDC 保管箱’的扩展应用图标。



单击上方工具栏的扩展应用管理控件，会弹出选项框，该选项框中也会展示‘DDC 保管箱’的扩展应用图标，点击即可主动使用应用，也可正常被门户唤起。



2.2 Microsoft Edge Extensions Home

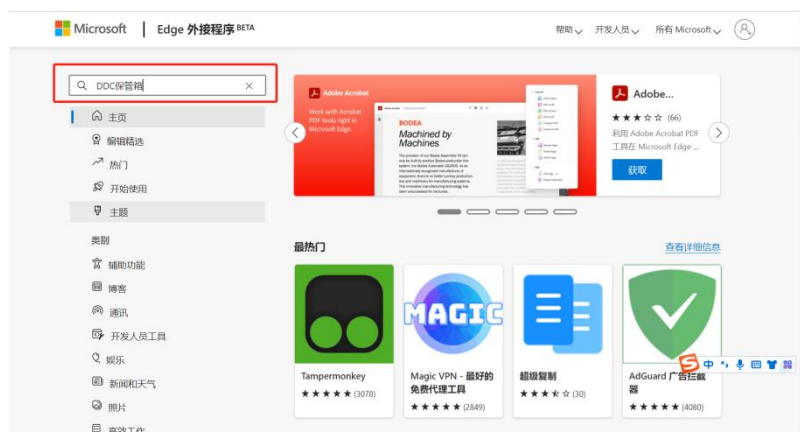
打开 Edge 浏览器，右上角工具栏更多选项中找到‘扩展’选项。



点击后弹出扩展控件。



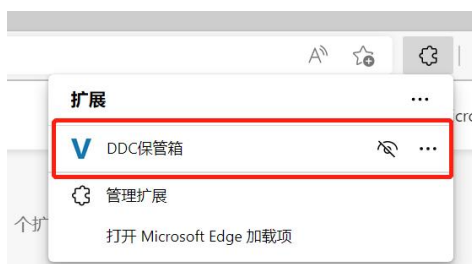
点击‘打开 Microsoft Edge 外界程序网站’后进入商店，在搜索框中搜索‘DDC 保管箱’。



在搜索结果中找到‘DDC 保管箱’扩展程序，获取并安装



安装完成后，在工具栏扩展列表里将展示‘DDC 保管箱’图标，点击即可主动使用应用，也可正常被门户唤起。



2.3 官方下载压缩包

官方下载地址：

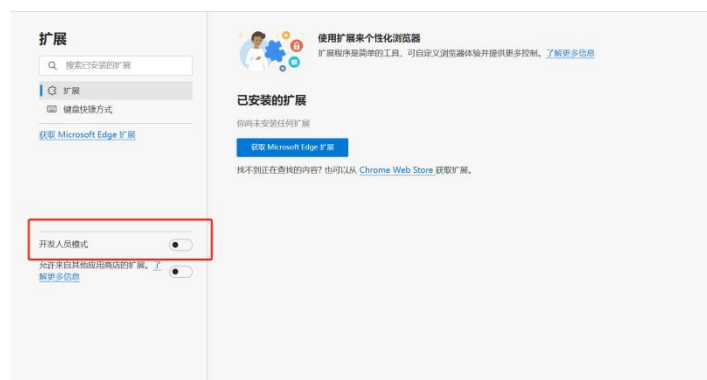
<https://bsnbase.com/static/tmpFile/ddcVault.crx>

获取 ddcVault.crx 文件后，打开 Chrome 浏览器或 edge 浏览器在工具栏中进入扩展应用管理页面，并打开‘开发者模式’开关：

Chrome：



Edge:



将 ‘ddcVault.crx’ 文件拖至页面中

Chrome:

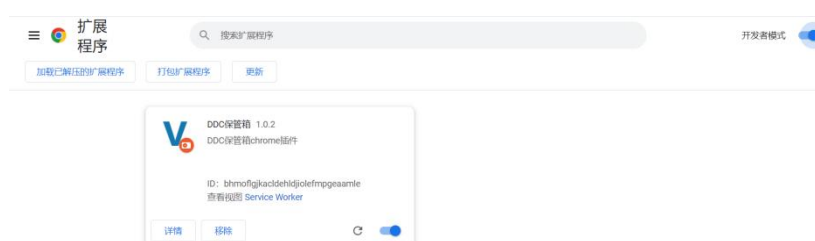


Edge:



完成安装，管理页面中会展示 ‘DDC 保管箱’ 图标。

Chrome:



Edge:



3 使用说明

3.1 第一次使用

主动打开‘DDC 保管箱’后点击创建私钥。



3.2 创建密码

填入密码并确认（最少 8 位），该密码将用于解除扩展应用的锁定状态，请妥善保管，仔细阅读使用条款后勾选同意。最后点击‘创建’。

DDC 保管箱不会收集密钥、地址、交易记录、DDC、哈希或任何个人信息。

DDC 保管箱不会收集你的完整 IP 地址。

DDC 保管箱不会为利益而出售你的数据。

创建密码

* 新密码 (至少8个字符)

* 确认密码

☒ 我已阅读并同意 使用条款

创建

3.3 助记词

助记词可用于恢复由该组助记词创建的私钥，外部导入的私钥无法被此助记词恢复。点击显示密语将可获取一组由 **12** 个英文单词组成的助记词，若对助记词不满意可点击‘更换助记词’换一组，确认助记词后可点击下载助记词，请妥善保管，然后点击‘下一步’。

切勿向他人透漏你的账户助记词。任何人一旦持有该账户助记词，即可控制你的 DDC 账户。

请务必记住和妥善保存该助记词，可将该账户助记词记录在纸上，并保存在安全的地方。如果希望提升信息安全性，请将信息记录在多张纸上，并分别保存在 **2-3 个不同的地方。**

记住该账户助记词。

下载账户助记词，并将其安全保存在外部加密硬盘或存储介质上。

drip report live pulp nothing vehicle
cram account resource girl jump away

更换助记词

下一步

3.4 解锁保管箱

打开保管箱后，一段时间无操作或进行某些特殊操作后保管箱会进入锁定状态，需要输入密码用于解锁，该密码为 [2.2 创建密码](#) 中所设置的密码，正确输入密码完成验证后即可解锁



欢迎回来!

即将进入到DDC保管箱

解锁

或 使用助记词导入

3.5 签名

使用列表中的私钥进行签名只需在列表中找到该私钥，点击操作中的‘签名’控件即可进入签名页。

我的私钥列表				
账户名称	账户地址	加密算法	备注	操作
Account_0	0x7448a31cf26f3ce986a0f4e78a511021f513eb6	secp256k1		签名 显示私钥 编辑 查看DDC信息
第1~1条, 共1条				

签名页中输入需要被签名的内容，并使用解锁密码进行身份验证即可获取签名结果。



签名

私钥标签: 0x7448a31cf26f3ce986a0f4e78a511021f513eb6

* 签名内容: {"to": "0xb4B4d6B2C7BC4389759f9EBE141cFE086771561", "value": "0", "data": "d0def521000000000000000000000000b898d0f"}

* 密码: *****

取消 确定

可使用‘复制’控件一键复制签名结果。



3.6 显示私钥

用户可使用‘显示私钥’控件获取某一链账户的私钥。



输入解锁密码进行身份验证。



通过验证后获取私钥，可单击‘复制’控件进行一键复制。



3.7 修改账户名和备注

可通过‘编辑’控件进入账户信息编辑界面。

我的私钥列表

账户名称	账户地址	加密算法	备注	操作
Account_0	0x7448a31cff26f3ce986a0f4e78a511021f513eb6	secp256k1		签名 显示私钥 编辑 查看DDC信息

第1~1条, 共1条

可对账户名和备注进行编辑修改。

编辑

私钥标签: 0x7448a31cff26f3ce986a0f4e78a511021f513eb6

* 账户名称:

备注:

点击‘确定’后，完成账户信息编辑。

我的私钥列表

账户名称	账户地址	加密算法	备注	操作
我的账户	0x7448a31cff26f3ce986a0f4e78a511021f513eb6	secp256k1	DDC保管箱演示	签名 显示私钥 编辑 查看DDC信息

第1~1条, 共1条

3.8 新建账户

右上角点击头像出现操作列表。



点击‘创建账户’弹出创建账户页，填入相应信息和密码。



创建账户

加密算法: secp256k1

* 账户名称: 新建的账户2

备注: 请输入备注

* 密码: *****

取消 确定

完成创建。

我的私钥列表

账户名称	账户地址	加密算法	备注	操作
我的账户	0x7448a31cff26f3ce986a0f4e78a511021f513eb6	secp256k1	DDC保管箱演示	签名 显示私钥 编辑 查看ODC信息
新建的账户2	0x8d260d3bf3ee039e19928835499a9ac94234a9f2	secp256k1		签名 显示私钥 编辑 查看ODC信息

第1~2条, 共2条

3.9 导入账户

用户如果已经拥有其它的私钥可通过‘导入账户’进行导入。



进入导入账户窗口，填写相应信息和密码。



导入账户

加密算法: secp256k1

* 账户名称: 导入的账户1

备注: 请输入备注

* 私钥: [Redacted]

* 密码: *****

取消 确定

完成导入。

账户名称	账户地址	加密算法	备注	操作
我的账户	0x7448a31cf26f3ce986a0f4e78a511021f513eb6	secp256k1	DDC保管箱演示	签名 显示私钥 编辑 查看DDC信息
新建的账户2	0x8d260d3bf3ee039e19928835499a9ac9423a49f2	secp256k1		签名 显示私钥 编辑 查看DDC信息
导入的账户1	0x7448a31cf26f3ce986a0f4e78a511021f513eb6	secp256k1		签名 显示私钥 编辑 查看DDC信息

需要注意的是导入的账户是无法通过助记词恢复的，请妥善保管。

3.10 通过助记词导入

如果用户已有一组助记词，可通过使用助记词导入的方式恢复已有私钥和账户。

填入助记词和锁定密码，勾选同意使用条款。

使用助记词导入你现有的私钥

* 账户助记词

.....

☐ 显示账户助记词

* 新密码（至少8个字符）

.....

* 确认密码

.....

☒ 我已阅读并同意 使用条款

导入

完成导入，解除锁定。

我的私钥列表				
账户名称	账户地址	加密算法	备注	操作
Account_0	0x7448a31cff26f3ce986a0f4e78a511021f513eb6	secp256k1		签名 显示私钥 编辑 查看DDC信息
第1-1条, 共1条				

本次导入使用的助记词与之前步骤中的助记词相同，可以看到0x7448a31cff26f3ce986a0f4e78a511021f513eb6 这个账户地址被顺利恢复出来，与之前步骤中的第一个账户一致，若要恢复[新建账户](#)中创建的第二个账户，只需要再创建一次新账户，下一个被创建出来的账户将与[新建账户](#)中得到的一致。但是通过[导入账户](#)导入到保管箱的账户无法被恢复，只能再次通过私钥导入。

3.11 忘记密码

若忘记密码，可选择‘使用助记词导入’，之后将执行与[通过助记词导入](#)相同的步骤，可逐一恢复由本组助记词创建的账户，但无法恢复外部导入的账户。

欢迎回来!

即将进入到DDC保管箱

解锁


或 [使用助记词导入](#)

3.12 查看 DDC 信息

用户可通过账户操作中的‘查看 DDC 信息’查询属于当前账户下的 DDC 信息。

账户名称	账户地址	加密算法	备注	操作
我的账户	0x7448a31cff26f3ce986a0f4e78a511021f513eb6	secp256k1	DDC保管箱演示	签名 显示私钥 编辑 查看DDC信息
新建的账户2	0x8d260d3bf3ee039e19928835499a9ac94234a9f2	secp256k1		签名 显示私钥 编辑 查看DDC信息
导入的账户1		secp256k1		签名 显示私钥 编辑 查看DDC信息
Account_3		secp256k1		签名 显示私钥 编辑 查看DDC信息
DDC演示		secp256k1		签名 显示私钥 编辑 查看DDC信息

点击‘查看 DDC 信息’进入 DDC 列表页

账户名称: DDC演示
私钥标签: 
加密算法: secp256k1
备注:
DDC总数: 3

武汉链

泰安链

DDC ID	类型	发行数量	创建时间	操作
10099	ERC-1155	10	2022-01-26 06:50:26	查看
10098	ERC-1155	1000000000000000	2022-01-26 06:48:56	查看
10005	ERC-721	1	2022-01-26 05:26:46	查看

第1~3条, 共3条

<

1

>

点击任意记录可进入该 DDC 详情页，详情页将展示两部分内容：

DDC 详情

DDC详情		
DDC ID	10099	
开放联盟链名称	武汉链	
类型	ERC-1155	
发行数量	10	
创建时间	2022-01-26 06:50:26	
DDC URL	--	
链账户地址	<div> 2 </div> <div> 1 </div> <div> 1 </div> <div> 1 </div> <div> 2 </div> <div> 1 </div> <div> 1 </div> <div> 1 </div>	

发送记录

发送记录

交易哈希	区块高度	交易时间	源账户地址	目标账户地址	交易类型
0x7b498aad2d73fe9ce3dbc2b6ecba9269f7997e04635a6e0616dd75c53c8f023	2088342	2022-01-28 14:11:36			流转
0x95a9b5c5305f42f952e62dd0b61b2becbafcdb6d1e621ed8ef96edcae8be011e	2088246	2022-01-28 13:55:36			流转
0xf1ee309e7a83cae0eb077b652e6be9f781f97dc7785f6063ba711d8f55949f1	2088244	2022-01-28 13:55:16			流转
0x076e852a19f2d31f164941e20589ce6b8b26f969b9a122273e79b3bca2ca0e27	2088243	2022-01-28 13:55:06			流转
0xf933df65b046939f9fbf295a189161c9e98421ac9dcc03189f3e8d1e83a228ec	2088241	2022-01-28 13:54:46			流转
0x59831c8c8691dbdfda93edba8753a5c2cebdf65a3686b64b676c4dbd0e044fe	2088223	2022-01-28 13:51:46			流转
0x23afd3ef2589351f86184972623ad5107f2de6ff947673700eddae1a0aea5ec	2088221	2022-01-28 13:51:26			流转
0x5205155cce056ccaded8afdeb7bf10a8105f1884dbe91905b64b804098b2ba7	2088218	2022-01-28 13:50:56			流转
0xe9b4aec6b119840b9cdf3499d694258141172241965f32672b6f5c698f5c990a	2068415	2022-01-26 06:50:26			生成