Web3 Wallet

合約審計報告

VER 1.0

2022年8月15日

No. 2022081514130

項目總結

1. 項目介紹

Web3錢包包括Android、IOS和Chrome流覽器外掛程式在內，一共有三個用戶端，主要功能包括資產看板、NFT市場和發現頻道三部分，資產看板提供多鏈、多資產的管理功能，可創建和導入助記詞，並允許用戶在一個介面上跟踪多條公鏈的資產組合；NFT市場提供NFT資產的一站式服務，允許用戶在一次級市場參與NFT交易，同時具備各類創新功能和靈活玩法； 發現頁則提供DApp、鏈遊等DeFi版塊的相關資訊。

2. 審計詳情

項目名稱	Web3 Wallet	平台	N/A
通證名稱	N/A	通證代號	N/A
開始時間	2022年8月8日	語言	Kotlin/Objective-C/Go/ TypeScript/JavaScript
結束時間	2022年8月15日	官網	N/A
Github	N/A	白皮書	N/A

3. 審計範圍

3.1 Android

ID	文件	SHA-256 checksum
Android/	WalletCreateUtils.kt	e86c771b5940c8284bd5b55769ae2808be71041357720d5d45742a1c1d7d867d
Android/	WalletBridge.kt	861af2d64f820dd837acb0d5f9e1312b99343a71ff74bdc8ec5a013f0091be17
Android/	WalletImpl.kt	ba9ed2f875fff6a5d828b5e5ddd4a1f661974d1fa71b84956881ffd17897b52f
Android/	WalletGenerator.kt	960cb05d2c653f5d1a00a22891b778852ae22efca973493a8e2305a14a3d12d2
Android/	WalletApiService.kt	6b65073531df9851c07826859d27488bce0c63a88795d4e7413483dc9ead6856
Android/	WalletManager.kt	434002140d4545b4bc5e05c597d565e94897369e5a73d47023e6e23120fc7e2d
Android/	IWalletManager.kt	f62f7d8f8d7d9d8ac8e1a21266d25a4f41c73f7a1cdbbc98593033b41fbf878f
Android/	WalletLoader.kt	9cebab782e3e14f1fa73bb24ebe56cacfddfb9207e0277180d28feed9271d87f
Android/	PasswordManager.kt	5bdc70d014ec3148cdd52f8a0f1fd803a85ea0d09344d906351f703e254a6d6f
Android/	WalletBuilder.kt	b9eb98b5a48704477b2fea801997f462648193ee57e22af40836cf862e0a3dd5
Android/transaction/impl/	OkNearTransaction.kt	2da86c5a63338ed7ee7ba6d334a6e3f8abd483e16834432ac4747fe9fe0b6d3e
Android/transaction/impl/	OkPolkadotTransaction.kt	74259e157130e010e9f2567772bd3aac5b9e7c688eff0e39e3be69828e6487cc
Android/transaction/impl/	OkAccountTransaction.kt	0e39ce5be8a630dba5b4a9fd27b2c7e6fce5cab6f09b26c3f100a5679fd91b15
Android/transaction/impl/	OkSolanaTransaction.kt	d65a3b5655b2d843fb6c4a99ef774c19a88579cbe9557dbdb6c16faaee334396
Android/transaction/impl/	OkCosmosTransaction.kt	597571b09b2dfe70b3577ed27d90a11ba5925c74ffcbcdd1236246731c9c3d28
Android/transaction/impl/	OkUTXOTransaction.kt	106fbe6e35d715514bccc9cbf3722ebc37de0a19371f8d5174a02f8410ebb059
Android/transaction/impl/	OkWavesTransaction.kt	a6c607278f4798ac5d1bb16b204bb4eff01617cb8d602df30068050fd8b7403d
Android/transaction/impl/	OkEosTransaction.kt	733d4629200a0bfae36c7b9bffa3ed484d1ae7a0ee71863157ba4cbcce8e0b71
Android/transaction/impl/	OkTronTransaction.kt	4771442acef494796fcee8966fb866fe04921852def5efd069efe7904454b454

ID	文件	SHA-256 checksum
Android/transaction/	TransactionFeeInfo.kt	6fe15b80bc21e9c84bec9b64b03348512845b51afe1fa2aff10fa03490178ad8
Android/transaction/	calculator/OkCurrencyCalculator.kt	b00906bb199b3783f3aab6146516ab69d321e04898b651c43aaad5e22d0b51e5
Android/transaction/	OKWTransaction.kt	afe65003b9a1ea39976713d5c14a91b105d5f2fedccebacf67e0461dde8d2479
Android/database/repository/	IRepository.kt	8f5067be6ef65c501b1c99abf3d020f6ded5007d2e56e4104dc938b16875a270
Android/database/repository/	KVRepository.kt	a5507044abb81cf046f94b4c788918087e0f6c020607775f24f4076174b5f439
Android/database/repository/	SyncRepository.kt	09aa25be018b723b39cccc4a0271ee469ad9fc03909b4a15281eeec2f03ea7f5
Android/database/repository/	AddressRepository.kt	0774645ace9891154d88ab1c50c01bea290e5e146128db9d6ba481276b318b14
Android/database/repository/	WalletRepository.kt	151996540cd108a7b6281914068f8c034f942494f53ac33bc08e5ffa75772fd2
Android/database/repository/	DAppRepository.kt	64179d021be8f4290dd3f6e512ce4cb7349c2956a283e3696c81fdef35b026a3
Android/database/repository/	MessageRepository.kt	f98c1dfc9d19afe983776d96eb325e0ea44f6eee309d91e6908b0c665b6e9cdd
Android/database/entity/	ChainAddressSegWitEntity.kt	ce5db3da451748456e03396e6c9857f610539a9806cf6d6b58edafbebdf548b8
Android/database/entity/	WalletNftEntity.kt	2541f89779eaca6cb24d6385120ac806f531769c6ca30311175255cc4149d878
Android/database/entity/	DAppHistoryEntity.kt	3db90fbf7157af472eb9bcf170653d054eba89cce2283d0078d70878f85b84b0
Android/database/entity/	AddressEntity.kt	5f4548f781d7c3b7851e70d1184299cd95ec05c1919b5e46335eb46b7f7fc634
Android/database/entity/	DAppFavoriteEntity.kt	a87e2b59b5c67350ac8863137158966d56224ea0d8883b406ed6d14c1d7207cd
Android/database/entity/	TxLogEntity.kt	3a2716d89e40058c92e44811f8398b7b182ee53baf1ced43f7366846226b2920
Android/database/entity/	WalletOpenedCoinEntity.kt	3bde25fe406719bbbd1cbaf1ee116cf3acb7f60c290b710422e57f29cd3ac93e
Android/database/entity/	MessageItemEntity.kt	104f7d29b4fd49b29dae972991d1b2b56bf75b3f246fe7a6713e3f8e134564e3
Android/database/entity/	WalletClosedCoinEntity.kt	f13fddb67d17a8a665e0e75636b1caa84220865606231a278a6d6270ead226a5
Android/database/entity/	KVEntity.kt	09a6b5e5f5cb7f7cde0c7d16eeaea68830819c79023c68bb5ea0c109dfc08cbd
Android/database/entity/	ChainAddressEntity.kt	0149c7b63a628c4c609b1f38e886ebe6df9d1342d086d5f333485d9383cd3554
Android/database/entity/	SepInfoEntity.kt	81c77f55cbdd4ea468571a6d4a30a9e9536a4879495d88829d430034b5fee667

ID	文件	SHA-256 checksum
Android/database/entity/	WalletDefiEntity.kt	90e3f4f8fe5fa12eb8d8cccc8e230ca0afc7febe54c71d62d0bb59351168534e
Android/database/entity/	EOSInfoEntity.kt	8419a4f0f80d07893d416bd876fa8aeb0ff4068fc06804ebc21d6d692bcae26b
Android/database/entity/	RootWalletEntity.kt	86347fdd4ad3b45b8d60874ec6f6e0aa3e6735079c09c1b5558766c71dd40912
Android/database/entity/	DAppTabEntity.kt	17ab9f59c4f7f98f786afbf3810cdc218324be49f4075580268c8febc207ed2a
Android/database/entity/	SyncItemEntity.kt	65104a2a18d26d070e53198efd6cdb2194c3af657689c926c341d44174faeb0e
Android/database/entity/	WalletEntity.kt	6f8ee8e0a1658c5c88c25689a45d3ef94af235d52994037ef39ff55be5d30e8b
Android/database/entity/	DAppSearchHistoryEntity.kt	0826043e924f4ec22416116dddfc6dd666e1672a773e9dac53677b65c73f7ea6
Android/database/entity/	WalletCoinEntity.kt	f8e5947a65ab8e172ddf02bfbe61c8d550b43c5ebd359746c8768b4c5875f852
Android/database/dao/	TxLogDao.kt	3d8f85287a44213cc6d0662f04068e090d9f96b211353e6d017fa7136f260ba0
Android/database/dao/	AddressDao.kt	5b2b478a98f8242c07352a0ebb6eab4d69248ece29807ad953229b7cd0bdb868
Android/database/dao/	MessageDao.kt	e15487959f8bf2732c0a05e6a07081ee4b38825d719cde98ae6602e501d431aa
Android/database/dao/	SyncDao.kt	5cfca79af0e7e2e518b32b1f3cb610e8752a9458c0a2e908659ef9af7844761b
Android/database/dao/	DAppDao.kt	fef8d9317ed1a8cfbe870233323c40471e87d67ce168cb5666a702d402055db8
Android/database/dao/	KVDao.kt	f6d0c456d1af9f6eb4f6b31fdc7a6ca9b99ebdc689bc1d1160186f4c08b31666
Android/database/dao/	WalletDao.kt	e32d5145ce7fa284f740d2a99f72a8c8f242c7b1d0f4af06bfe837f14def4cf6
Android/database/utils/	WalletSQLiteOpenHelper.kt	04e10b3afe29b1d4426c4f117fbeb73063db650ea50d99176f3339bf5af13b0b
Android/database/view/	WalletView.kt	f8c15d54f33a4e03bfa3993d1ebb2d4c91b7037e7d710165526766620804 0af1
Android/database/view/	ClosedCoinView.kt	16a0d9142e73346f37a8a9c3ba72bb0481bf06de1382d80743054b6ef00c8429
Android/database/view/	JoindChainAddressView.kt	f0b47ee031685465fca2551b4943fbeedc44f05259c0f18acfdeba143f7c633d
Android/database/view/	JoinedChainSegWitAddressView.kt	49d3ebda733473f59a3ae09db9b3ac234a306ec3bec1d7a2639d1af5696e6cb7
Android/database/view/	JoindCoinView.kt	ba06d04d4bc1ec38f2cf47fe3a2ca25549101e34e46960512d3ec769cdbfd938
Android/database/view/	JoindDefiView.kt	b42a35aad33e2afe9ab8427cacaec7b58b58779d6ab5e3af7af0e0a015078f5a

ID	文件	SHA-256 checksum
Android/database/view/	OpenedCoinView.kt	c48fce55152529d27d75f9110328139c299ccedc26235be624c4b0853a5f6267
Android/database/view/	JoinedNftView.kt	b95c02416042084818a78f421c3b5bb4b3de70aed050438444c2a3db885c9eb7
Android/database/view/	RootWalletView.kt	f3d02505789a855d1e3a59e350d1509e07e9c742adac6d01aeaf0b6b5d3d1cde
Android/database/view/	JoindSepInfosView.kt	b119740b4e2b698a754036277defbbac3fbd55e597e3a8b1b29c5696d52a7a28
Android/database/address_book/repository/	WalletSendCoinRecordRepository.kt	5ad5e18235a95c29c78f300a567de00516fa393d01fa835178fe031a0bfd6227
Android/database/address_book/repository/	IWalletSendCoinRecordRepository.kt	b8774fa89dbeda604423ca566c047cd34ee60ca61df95215a5cec6323ae98d33
Android/database/address_book/repository/	IWalletAddressBookRepository.kt	33e87adb1d5d81dbbe744bf085205d11b2a7c429528b89f91b27520653d05bef
Android/database/address_book/repository/	WalletAddressBookRepository.kt	a9537ecaee6e7ee6d8e368dc1dfba965bf7ae7c0c503471b846761beb3fe2e2b
Android/database/address_book/entity/	SendCoinRecordEntity.kt	9601159b2710498b0470660fd13bbb3db671b72ef7bf01018ed228d0858a58c5
Android/database/address_book/entity/	AddressBookEntity.kt	351a387e9fee8b276a55b9bc4e612828d35f3164227133cc2e8a6314132272e2
Android/database/address_book/dao/	AddressBookDao.kt	4dd10278a6929b99826fa8be0e7f2b71e3f8dbff5edd95dc1198df8baebd1196
Android/database/address_book/dao/	SendCoinRecordDao.kt	6849858090acbe5ef6ba9c55a96aa6a654cb6534ba264955a116d87a2441bd61
Android/database/address_book/	WalletAddressBookDatabase.kt	91ff11ab4d2fe70fd0b6779fe4ff697d683682b2acbbde72020fb859dde7ca3f
Android/database/address_book/	WalletAddressBookManager.kt	48de3c2d2b345bf614496fbc994bfdf164842e6ab5d2b33b8d16d2cd2d0ad9b9
Android/database/address_book/	WalletSendCoinRecordManager.kt	0aa2d3aa95c45bb7ab959879ce881b0302073c6ace322a3e2b7713d09172097c
Android/database/migration/	FlutterWalletDBHelper.kt	bf69ed240ef230d70a64ced7fad3e1c129eaf5ca523bb903fe94879be1385e58
Android/database/migration/	TableChainAddressMigration.kt	643b454473e39dc9d97e9c40f783c0b50e6b20e15126fcd9ccd403bf45c7aa57
Android/database/migration/	WalletDBMigrationWorker.kt	eb0d645dd11dd503b5b9f533353829d15b39f4f72a667eab62c42d39a65328a1
Android/database/migration/	TableMessageMigration.kt	b3b686d3808c8c941e8c3026b3c49643074a814daae35c6002dc2cb85ade1cdd
Android/database/migration/	TableAddressMigration.kt	458259ec8d82a09a2c16a83e530f8a7471bb9b706fe018c3dcc4b015009ed052
Android/database/migration/	TableKeyValuesMigration.kt	dfd93c1c4332ea2d577224585a4571aa0dc97ce078ee3dab9fc4807d362a64fa
Android/database/migration/	TableWalletMigration.kt	2d50b529973b80f68f847588fd346b4859cefd5113e08f46af90a228d19163a2

ID	文件	SHA-256 checksum
Android/database/migration/	IMigration.kt	b321b664bd793d08b6368a8f68856634185aafa170e575296694959ac6262c2d
Android/database/migration/	TableSyncMigration.kt	aa63e79f2ece5484bb6a9949577265d4928b2e18184eccc64d8061c5372de6d2
Android/database/migration/	TableCoinMigration.kt	5d650d47960ac133f678ad9aae1dffaffc33b41cb7add2812ecaa6bcf837c311
Android/database/migration/	TableSepInfoMigration.kt	6ab55418551ea6e715df4f019d54a01ee69243e0b1a245b48e07c2bb1f93c5db
Android/database/migration/	TableEOSInfoMigration.kt	2e942552272635a755280747992215629ef9c16a3d079fbccab8b7ec6c95332f
Android/database/	WalletDatabase.kt	cefae4dda49c30514f5a4217b81ee432252b3b4090b96419ddfcfa02537594cf
Android/interaction/impl/	EvmDappSignInteraction.kt	f9b707aa3cb842b8fcb194f627f65ee6b6f06c0e0fd072f248f7ed9d7d2c3917
Android/interaction/impl/	SolDappInteraction.kt	0ae97a6abba80dae9eb144b9c90ac61e8384b0d796c81886d2186ee63f938eb9
Android/interaction/impl/	TrxDappInteraction.kt	218754c74ef5e6ea555276bb939874852fd1debc5fd6e31b325722420540b111
Android/interaction/impl/	SolDappSignInteraction.kt	70610940f3ce0f1c4f4305dca29924b01d201d15e0d255c8e5956e7135d02d9e
Android/interaction/impl/	EvmDappInteraction.kt	c970aa2171be3d3c00cf2efcadad9b91ac7265c3f269679b55fbc1912a0b6b46
Android/interaction/impl/	TrxDappSignInteraction.kt	3dd4f81629267822a1f03ea2171922fb32ba70115a8ec197dc84bda58993d62e
Android/interaction/bean/	DappSignInfo.kt	04af801b85530ccd79fc9bcce15c0864faa49c639f2c8d05875496af4870a633
Android/interaction/bean/	DappInteractionFeeInfo.kt	b460b9db8cea9094db4b19f1158fdd48ba865590a35012a1337e6ec254c660e9
Android/interaction/bean/	DappInteractionResult.kt	dfe112a1e7749c75de60e505b82494be2bd9e51d7d415568f14e4b4caf0be396
Android/interaction/bean/	DappTxResultBean.kt	9ad1d138e26ebf84db6a427655f8b741218b361b16799132e25ac8fdf37a9376
Android/interaction/	DappBaseInteraction.kt	350a7fe333bc4b6d3c37828e06e055f3af5155478081a230076ca3ce58aec602
Android/interaction/	DappBaseSignInteraction.kt	cb11ddf60881bfdc7023300ba05316fd256ac76ed967934ae2c863cd065297e3
Android/interaction/	DappInteractionFactory.kt	3cc22bd528efe5dd869553e2fdf8499a12c7ed3f370bb3b9e794791f5cb10a26

3.2 IOS

ID	文件	SHA-256 checksum
AFNetworking-4.0.1	AFHTTPSessionManager.m	b74fcb9cdab6f88689517d7677650db114288f0cd7d1794e3d4175f43821dd5e
AFNetworking-4.0.1	AFNetworkReachabilityManager.m	1cd57348a69a4faa6c1e0f8facfc95530c48f93c7a544700cb6542b647a1bfda
AFNetworking-4.0.1	AFSecurityPolicy.m	1e942f9bcf388b59c7f6a6440f332ba8dd3eaad93ac24854ed29913993926466
AFNetworking-4.0.1	AFURLRequestSerialization.m	4b84420558443275 93d5025e18e6fdde860309e6c12d71f28673ba2cf2d9d190
AFNetworking-4.0.1	AFURLResponseSerialization.m	a8d3826d2046ee693e80c4e318cf3e5a4b8396c35479dc1025946932e19e8918
AFNetworking-4.0.1	AFURLSessionManager.m	9e3db7d740358ba0e5fedfb70747eb8b2bad9ebb744fd434e129f4347906f906
.	OKBAsyncLoader.m	6ac6b5c81c44b66c0cf816eee3860971ece90df55949458155da9a7c410d0d39
.	OKFAPIBaseManager.m	b0a8aff8e98cee5f7b69395508c1669bedac8908ab24b41abb71545ab4a39391
.	OKFAPIURLRequest.m	c9db82d6dddc854fa32338a7c7a6426474d9086aac2607eabcbf8b520cc71eb9
.	OKFAPIURLResponse.m	2dacec3eb0b48131ccb4eb6745a738dce558ecc6df8d0e26dd5aad7da8975210
.	OKFRequest.m	dd22f8733a79cf35fadeefb15a6384a92950200be8ff5e5eaf8128c5bc6e2c32
.	OKWApiService.m	b1b08d1ea4080dbeb3dad3db0e7a5400790a19f74625ea1d2280a31edb7e3f66
.	OKWBridge.m	8a6046baa0db943c17cce628bad850931ddbe0f243ccbd7d0c166873ac769196
.	OKWDataBaseManager.m	e26c013f801e1f414016e7c89bdaed2035672b7c52066d102cfc03c9bfbc3a2a
.	OKWMnemonic.m	8f48f85015ef54c968034bb54f3d1013039906ad8823b4e3fa404227abcb8872
.	OKWSchema.m	87d2781e32077a8668238d2c88bbfb0973574f2e636286b09f17b74287d13f08
.	OKWWalletManager.m	df9c223cb420df4cda061a4d3f314a3c93e959507af90631bac22370051fa951

3.3 Wallet-Core

ID	文件	SHA-256 checksum
Wallet-Core/build	gomobile	ee66cfa3fbe19606515f92cdf3c8c9118ac49799d7f0883ed6780121f0df5590
Wallet-Core/build	index_test.go	7e1f0717cc427bb6462210e50e17ba86a9c7fda60512ca5ebc9df53edc410821
Wallet-Core/build	index.go	3ffa7f07836b18e9ce19aca8ec13fa24c09bfdd657eca2b8477616758cf2adea
Wallet-Core/build	makefile	ff6d1bbf9af2d7128134ffa7ef4d5ca92d8090aeb9d8cdae2ff778f30aa6fa78
Wallet-Core/build	nft.go	7c79bd4439c8aadd76ee10cb172126fbd7e9c54de3f549975972e6c58f174484
Wallet-Core/build	patch_286.go	cbd8615750b818990426821e0467f00695b7a8e35fce6ce694ce7f87e725b1da
Wallet-Core/build/test	base_test.go	40b316f8e15d476ee6486a4db6299bdb6d2c3c1767fbe26daa4194b0bc5eebf1
Wallet-Core/build/test	cosmos_test.go	460a636e4618fe06500cf300273c80b900e1f9d77e601ec7a4bbe30d84acb8b3
Wallet-Core/build/test	elrond_test.go	6ec965de2881e6684ce66ba8717de45846d49932f122b1c9f298891d5af44e34
Wallet-Core/build/test	eos_test.go	54133c5536563812011641746753ca8fbb61eb1fe43ed811486e5debd90916d8
Wallet-Core/build/test	harmony_test.go	3abcf03be631aec78c1e9a70c918f11f29947885088989b1df365b335d061f94
Wallet-Core/build/test	near_test.go	3abcf03be631aec78c1e9a70c918f11f29947885088989b1df365b335d061f94
Wallet-Core/build/test	okt_test.go	eb339f68cdf6150eb1c2943b71116584ea612ee28bf134a9eda817ac14ff56fb
Wallet-Core/build/test	polkadot_test.go	f260de088d23dbc86c609a3e92ae111a6d0533d2d2da29740d4f579408475eb0
Wallet-Core/build/test	solana_test.go	03dc078611b80a289ace4aaf6c3cdd248a0416cf885f37b2c6226805cfe2049b
Wallet-Core/build/test	starknet_test.go	81be78f9eb80bd8b0622e8f8a60402f382edcf31edbeca3831eb2c7155135bd4
Wallet-Core/build/test	tezos_test.go	c3ddca2c76d711cd91147b9ceea031709bb280fe07a59a99547e91bf8e5aaf94
Wallet-Core/coin	achain_test.go	e749b81b33d20078cba185231abae6e3e5a628dd2d310c1a749d42167cad5e87
Wallet-Core/coin	achain.go	154b2bf85a4d4a86b3165a3af0600079d517ae2493b90ab670abe1e3922196d9
Wallet-Core/coin	ark_test.go	727cf665d0e03e9537a0a892cbea530d058b339cb81231684708d170b34146cc

ID	文件	SHA-256 checksum
Wallet-Core/coin	ark.go	afece9ef587d0f6cf72ae6ebadb2e10229c7c8a17fd6f5564022378cefaae2a9
Wallet-Core/coin	bitcoin.go	457ff99eaee63427b84a3c9fe68c4cc83fc1700e25000d3d761fd740daa81cc2
Wallet-Core/coin	bitcoincash_test.go	3097233072c2f9d6dcc8473c9e7c587581c86e51602b593cca14c18b978e50a3
Wallet-Core/coin	bitcoincash.go	7929cdda6272aae54ed8abf907e128cb923c328998a7121a204dbff7837a4635
Wallet-Core/coin	bitcoingold.go	559c4875cc4080b651eab933c183aa49940676eb7513f9ccfdd1ee119db6fd08
Wallet-Core/coin	bitcointest.go	6b3b158d5cc489fade6ade561f51329bf9e2b839f352f74ac68e8beb45e13a7f
Wallet-Core/coin	bsc_test.go	30d94cf380f2ce7855d211bd9d40f8e673d174734e83e99200fca3bd376df501
Wallet-Core/coin	bsc_token_test.go	5e5185788a6b4609e764e291947a40d03ee97ebf4813825a159d24becc78a3e3
Wallet-Core/coin	bsc_token.go	dd26252e7b27e894919f439dc386f253be6b43b39897439b916b18c79d3559f1
Wallet-Core/coin	bsc.go	0b154fdc3654a36025e7bcc2b4a3eab6a5e67223f7007a5ce988dc7392622ed7
Wallet-Core/coin	cosmos.go	ceb481b89427455046a1383ba3772294523ac4b5bd473f7d04f8d72fce6a3cd0
Wallet-Core/coin	ctxc_test.go	a0b3bcfcb50acd31bb6d6be48169cc0878646b5bd38eb86ea96f36a272e0e12b
Wallet-Core/coin	ctxc.go	0b0563f8dedbf2bc0017256613a327b4a6fc7f89c7e2ee6887c1d5fcb27ddf6b
Wallet-Core/coin	dash.go	0db7809b93a11a052e0d3eeb78ac0cab494c4ce0a550bd4de6da79087f012991
Wallet-Core/coin	digibyte.go	3123be0798a7fbd7ec27c97f7a95aa2375fdfced9e6ab2424e4b70f38a7911be
Wallet-Core/coin	elrond.go	8f19a2b8370c9e3dbb56acf9a9610b7c7a0fed4c675fe8fad33fe855aa8d1f7d
Wallet-Core/coin	eos_test.go	908215706ebc31cf44364a1f36c15cbddcdf8f032a2314e19b0eb2b046151c65
Wallet-Core/coin	eos.go	d83ecfc56303c0371892c010eb8de51e4e1be6ded9b94a1dd6893ba48f5278a8
Wallet-Core/coin	etc_test.go	08e36bd0a66dc49d124062b6a3ce1546ce40149a9b3ed384b1b0db59d27dc292
Wallet-Core/coin	etc.go	781d2e0f83d15d0751e09bf04835fe9bd7e0977a0c64dbd304c06b4968a5f4b8
Wallet-Core/coin	eth_test.go	6460f3595816e7cdb660ec3aa572bcf23d68f493b0bdce2920ab8c7e20cd79da
Wallet-Core/coin	eth_token_test.go	405930954fda77b026649dae772254bc91e529dbb6bb21059883f7c81e91a35c

ID	文件	SHA-256 checksum
Wallet-Core/coin	eth_token.go	9c6d6a73318c8ddf79091a7745aa83ffdb18582880f47fd98005145a0cb8f197
Wallet-Core/coin	eth.go	20f33a4ddc29e89771cbe8bd39e8ab96c37090b9018d8dfa5da3af113e39c605
Wallet-Core/coin	evm_token.go	1d424ffc5e5e27da0850ffc335b8a94bde144c13afd44514cff68f415b4cd3bd
Wallet-Core/coin	evm.go	aea0ef9d95beb9fe14ef9532f7e5ae12b7ba9e16fb71e27980f846da4ac01146
Wallet-Core/coin	evmos.go	f3ac8bd896dfbd7cc6df9ccda90fa364b0a8423d94ea5b1af1f07559f92f6b8b
Wallet-Core/coin	flow.go	6460f3595816e7cdb660ec3aa572bcf23d68f493b0bdce2920ab8c7e20cd79da
Wallet-Core/coin	harmony.go	f3ac8bd896dfbd7cc6df9ccda90fa364b0a8423d94ea5b1af1f07559f92f6b8b
Wallet-Core/coin	icx_test.go	1ee1ff63585b007d6f4575ec7db9a01101173b84412f59e3d074dbd10b293acf
Wallet-Core/coin	icx.go	f428e5ad5974e54ffbfc8b18cf531f3a773b7d907aaf8e74eae7e8c68375efa4
Wallet-Core/coin	litecoin.go	3ad494b602a5240c02ad3c132439f987e7031e4473dbef4b943c6268323296ec
Wallet-Core/coin	nas_test.go	db4774d12167486e1910edfa392ddd63c82b96f5835c64e8e1752d5cfa3cf693
Wallet-Core/coin	nas.go	6bc7620159348a82ae9d7f87c09f4549abb3ddfeccc8a6dc10ccf1dd2ae7fd91
Wallet-Core/coin	near.go	c391344cdcabb8d65b8b89f6a283388770ac28a3f3ff44cf8980b2904bf3a72a
Wallet-Core/coin	neo.go	2e53579ac1fa36b9ba29ece552db744bdfd1f4b14cc8b2bcfecd5f29e6b57fcc
Wallet-Core/coin	okp_test.go	4d6423f4c1f552b1dae6b198b2ddaf94ca24d4f43bc43d274e281ef3b0dae4b5
Wallet-Core/coin	okp.go	288d805ab307181410c78ea62e0a3085e153a5418ba13456093079b4ae56d6b1
Wallet-Core/coin	okt_test.go	3105bb2fde1e87626f27f74536a343d80ba321b1b99294682d8c86cc66052278
Wallet-Core/coin	okt_token.go	4080bd1b633549b6a0a4cd45aa9432c10a43bf4b20e401a781e8be2f46870d03
Wallet-Core/coin	okt.go	0ad559610dc8aa80aae5af5fb8c635e671141da7901d4134d743ebd463b87495
Wallet-Core/coin	ont.go	3e131f419d88df024f39ba22eac303245cb82e6e599f41e65235be38178448a7
Wallet-Core/coin	polkadot.go	4970ca63c6b391a49c32b750111d24205acbb33b1a563b07a81ffd41e2430038
Wallet-Core/coin	polygon.go	c90f2f6e401216526cce9c076030ebaa623297f9f6fceef5c7c7d038082de4c6

ID	文件	SHA-256 checksum
Wallet-Core/coin	polygon_token.go	62eec4d805af28133824a185aebeb5e9698f0b0feb92deed39250c21268c431a
Wallet-Core/coin	qtum_token.go	781649f31d0f0bb5da2a27a718de5515252fab6184022ef10f3a3daf66332113
Wallet-Core/coin	qtum.go	404add648b68c66b254589c21b54304209ea4617d83144906457cd10b4506d6a
Wallet-Core/coin	ronin_token.go	621a5ed0858bfde11cca9466621af1ec2dbeca57cb408f367940a10cea3f5207
Wallet-Core/coin	ronin.go	ad2969431ff5bcb7e8ff624a18fe12c4efcb74cb4cdf27ab7a3206fcebb5dea4
Wallet-Core/coin/sign	dot.go	1b762f58bd03d428a35313de5e10755474ab707867c7c8d6e41c74d489698593
Wallet-Core/coin/sign	eip712.go	dfbf6944db7c4caa8c847521e939a49f54869ebe2971c076454c81c9f0d16701
Wallet-Core/coin/sign	eth.go	1e76c21802163c74de1da144274fe57c1d57db0a5213234203de8684a04cbbde
Wallet-Core/coin/sign	op.go	3aae434803a5741e324b32505066b60ab6c959d1a2c89aa35569d33b5f65f222
Wallet-Core/coin/sign	tron.go	ad4949a1401afbc791e59b909c9b3ba444bc68a42b238aa99d1a012fc15aaf80
Wallet-Core/coin	solana.go	57380e9740e7f5dcf44828f9991ff6f3029b399cd1f3876393af081c48c1c78d
Wallet-Core/coin	solana_test.go	03e3947e27e5cfa86ca74cdc14b21e3b5fffb9f1122ab046611b47136e40ef10
Wallet-Core/coin	starknet.go	ea186ac4313436b5cfeef8438ec80bd0fcb98242dda3cd221f68d5e1e6938c3e
Wallet-Core/coin	starknet_const.go	f34cfb5d439a032dd576322e99a8762069bbf5904296b8f15ffa3663dc2ecc5f
Wallet-Core/coin	tezos.go	0f787edafca45109e75d3c5d58f96300caa987ed4f313c1c983a218912a7584c
Wallet-Core/coin/transaction/act	act_tx.go	331a97c5fb7939c10882dc4793e3d21a3c983bca39210f83a0650c9e34a5811c
Wallet-Core/coin/transaction/act	act_tx_test.go	dc328fad88783e18e49f9e31b9167a16d70685ebb159b370b6f3d7cabfb62685
Wallet-Core/coin/transaction/act	condition.go	7a1ab903a54a7ec1b0b042120090090158e92c78bc827c52d1ee2b8bb199d2aae
Wallet-Core/coin/transaction/act	condition_test.go	98d40c0dc73a4848b586e63a10fa18f0288abcf840697c9f5231c84db5969c4f
Wallet-Core/coin/transaction/act	encoder.go	783bc909db77fdf4c64d28df650ebdc28b2ebcde90cd10c32f6cff1d00b2d292
Wallet-Core/coin/transaction/act	encoder_test.go	98d40c0dc73a4848b586e63a10fa18f0288abcf840697c9f5231c84db5969c4f
Wallet-Core/coin/transaction	ark_tx.go	6939be53685ab8abd55027f6ec55e709d9b3a5795c574a606f224473df7882ed

ID	文件	SHA-256 checksum
Wallet-Core/coin/transaction/bch/bchutil	address.go	7992ba5f221035275eb365eea084c620607c7e5c45bf1432176dea090f40c77b
Wallet-Core/coin/transaction/bch/bchutil	bitpayaddr.go	d78dfbdd66ee7c95be23f269a0eef236bf9a68699f13bad5b70530979d647cc5
Wallet-Core/coin/transaction/bch/bchutil	bitpayaddr_test.go	4c082b84e03fa01fe26eae49119729c51cdd5a1d8fd5ae501298075ae7442266
Wallet-Core/coin/transaction/bch/bchutilWallet-Core/	cashaddr.go	4c082b84e03fa01fe26eae49119729c51cdd5a1d8fd5ae501298075ae7442266
Wallet-Core/coin/transaction/bch/bchutil	cashaddr_test.go	4c082b84e03fa01fe26eae49119729c51cdd5a1d8fd5ae501298075ae7442266
Wallet-Core/coin/transaction/bch/bchutil	protocol.go	f60523c277d7dad431d926c6f36cc4249c234cfc45be8728516293d730eca30f
Wallet-Core/coin/transaction/bch/bchutil	seeds.go	f99f384263bc56ef8763391a1969bbf70d558dce608abb14107a5c2c95b8b7e2
Wallet-Core/coin/transaction/bch/bchutil	sign.go	0527828ca260ed0011bc86689d22c1fb4b914a8411454cd564c13eee18ccf84b
Wallet-Core/coin/transaction/bch/bchutil	sign_test.go	a027c72c16d134f6d9514acf021ad0a0f4d1d406b9473c4441f2dd8600b0fa85
Wallet-Core/coin/transaction/bitcoin	bech32.go	c901827c57ef8ed54dcd1818694ef2273a17a60f01a01132b67c993e19347d12
Wallet-Core/coin/transaction/eos	buyram.go	151b3e23351d208557f4d0726296b7d3cf067b3fe9f7a617518a1f9321f24b81
Wallet-Core/coin/transaction/eos	bw.go	11e98e5e300cc8e93c4d9bb3db99e5c61153c29ac75c7c75028edd9514a72e3d
Wallet-Core/coin/transaction/eos	decoder.go	22d5400bfdd19fd716e6df98c9ddf7f7f88101ba31e89009ab229da4af5a850b
Wallet-Core/coin/transaction/eos	encoder.go	51b8b786f0ed76193b7f4aee7ea256f5e83815ef036f1cf34b491e9ccd0a66ff
Wallet-Core/coin/transaction/eos	eos_tx.go	70310e17b1b40a7af68813af64042a00bfe9a7fa044fea6bb7fba7ad479e0d85
Wallet-Core/coin/transaction/eos	eos_tx_test.go	e17cb486092aa543c9b22721d54bb0754b734797949050daea0cd1b58a883421
Wallet-Core/coin/transaction/eos	name.go	d63a5470cd1777fe931601f68a99ecd68db481aebb29d23cb42cf87f7aad8887
Wallet-Core/coin/transaction/eos	newaccount.go	094dbcd3878727e8fb7f47534aa396a789bd9d4f8cd10d7d492b3ea5db35a83a
Wallet-Core/coin/transaction/eos	pubkey.go	1536719639950f7b9a9252e7732118cc38631c04641fee722aeaa2fce57dbb8e
Wallet-Core/coin/transaction/eos	sellram.go	e889e57b66ed3c0186cf4d962dfe0920bb8af7bdb8696f9294a1fcd0ec32659c

ID	文件	SHA-256 checksum
Wallet-Core/coin/transaction/eos	transfer.go	4d3b201b1869cacba8de9efca4de65ee9006ae65ca1e608321fb163bb8f8e095
Wallet-Core/coin/transaction/eos	tx_factory.go	e04d693bdb6888c94613237b0421ced13eb64a3bb76d8ccd1de92a287202f76b
Wallet-Core/coin/transaction	eth_tx.go	727a90af04be96f49739e8dc930fe3f7d5dee2194349627f1d8376394344f782
Wallet-Core/coin/transaction	ethsign.go	7e9689f07aced6922585016b848298976bc3405f4387a18509af9cb3022e83e2
Wallet-Core/coin/transaction	icx_tx.go	9e65e0ac861454121eb9463f1f4fd826b4b7a7a7c87d7381c5e52693819be9ef
Wallet-Core/coin/transaction/nas	base58.go	15b9c045335a659611ade5d1e3b2bcb4fd9519164ec56c447f736365521e2409
Wallet-Core/coin/transaction/nas	block.pb.go	2b971c09b6646220ef97f92f2c17199301a24df0c71bc259bcd44e7c8d892fe7
Wallet-Core/coin/transaction/nas	nas_tx.go	d86ff34e522899c50c7dce7c983bc7e9c24d5768efb89a6f20d2ad830b2b0232
Wallet-Core/coin/transaction/nas	nas_tx_test.go	5d2caf3748466b1deea16af77e7e4bbf7ce0dafdd18c21a00bd04bc5af3ba199
Wallet-Core/coin/transaction/neo	bigint.go	7a00bd2b5772f2870a83f55455e772310cd0a7953fb60edb521ed606f4202808
Wallet-Core/coin/transaction/neo	neo_tx.go	12acb3fdb9016633446c31b1eab14d71764db76b3839b96da56a19a860aa6d59
Wallet-Core/coin/transaction/neo	opcode.go	1782ab0b3e3e8463079e46337e2a659532a7dcda4bcde95856c42fc99b6eafaa
Wallet-Core/coin/transaction/neo	params_builder.go	ab1cd66adb7a4f7cd810b11e86811929f8d11bd915ec909a91552f80bab69b02
Wallet-Core/coin/transaction/	okp_tx.go	05ae27e0a2a0ff0b68da4df351065ee1826f2479ae8a33b0c8b6680ad6bf1f2c
Wallet-Core/coin/transaction/okt	address.go	36ce0dcaf56a915c25afa676f5d19f7516118e962f778f1468339d4ddf9fd3da
Wallet-Core/coin/transaction/okt	codec.go	ab51a5411e78f93f7c187976143e32abb1abaf24f0abc506a93dae15b6e46d6f
Wallet-Core/coin/transaction/okt	dec_coin.go	9ff8efcc5ae903567a2d83b5ae75ff9c2f24053f87dbaa84616b8cde721f7ecd
Wallet-Core/coin/transaction/okt	decimal.go	e7628968d6d6056bb87c30dec423dd23b5615d98357f72de971e4ae64e31da1c
Wallet-Core/coin/transaction/okt	int.go	6d2f049156828dfbcbb5cd16651ae9a2ca79127b0bc349656bc62ac5018629f0
Wallet-Core/coin/transaction/okt	key.go	19447ac08641c8bdeffc2c10d71a9f92700d6e80776b902fee087afc2c95247c
Wallet-Core/coin/transaction/okt	module.go	aba40117bcaae1d180cef0ede60b72c4fa74f28808193dbff196a05cfc1f6121
Wallet-Core/coin/transaction/okt	msg.go	b6d2b55d33664a2638cb12447b12f90a8a72682f170f24e3818af5b070182b06

ID	文件	SHA-256 checksum
Wallet-Core/coin/transaction/okt	sign.go	a74338c1ce0dd79badeb11c8a998292dfb96ea3b71d0b0a05cf18723e1e58660
Wallet-Core/coin/transaction/okt	std_tx.go	15c7f5f8dcb594dd5e30477a2bb35463c9bc39fd74fddc54d4296562c4fd2b1c
Wallet-Core/coin/transaction/okt	stdsignmsg.go	25d09f026b9b63290028849d2325fcee6fca763746714b1c0ef77b05a822a2bc
Wallet-Core/coin/transaction/okt	tx.go	db257018bb567634f9dddfca3cd699f45b00c90e688800f2fbb0556d8aa1c8eb
Wallet-Core/coin/transaction/okt	tx_test.go	18746365c361311bd2395808ed908de0406143953c0219f85eed95a29f4141b0
Wallet-Core/coin/transaction/okt	types.go	046ef8e7efdb167ac9f2ca734d071821bb0e7072e952395ece79cbae5b1ff8d7
Wallet-Core/coin/transaction/okt	utils.go	acf6a000aae34954fd27143d278ab6e124e9a55e17a827ede62eebf175b294b7
Wallet-Core/coin/transaction/	ont_tx.go	de014e05abec0d0ed2ee9e7b67be0cb5728aa2ecb3bd507cac2fe34c9fcbb54c
Wallet-Core/coin/transaction/token	abi.go	6c9047045cec5982aab045a17eda92f03892d069fc7ab6ab23724c393f0107f4
Wallet-Core/coin/transaction/token	big.go	9fe14d3310ebab4c595c60659ff59e1a92e86d616886a8ffe5b2b11d0ef4d980
Wallet-Core/coin/transaction/token	ethtoken.go	67d4f814d3007865313a4baa5feefbf07d0cc3495956bd9617d9033c45814d34
Wallet-Core/coin/transaction/tron	Discover.pb.go	1191cfbfbbc13083414b5296a8a0c4371bff546bba0bed0cf7092851fde68f37
Wallet-Core/coin/transaction/tron	Tron.pb.go	cec98cafc6cb1419f9e09284534176ce32e512e3f083487b4e9f53ca6603eb0b
Wallet-Core/coin/transaction/tron	TronInventoryItems.pb.go	b99e48fbedd52126888fc4743d07e41aab7eb67a71c04e027c720ba1903923d5
Wallet-Core/coin/transaction/tron	account_contract.pb.go	b2632d18c42b6547dd46a0078a56aff923c6bc9ca66e79673bd9cc6d9a6f6f6d
Wallet-Core/coin/transaction/tron	api.pb.go	f1e858706afe14163b31226289a4b9cb7860d2895bc150fed630bc15ef839632
Wallet-Core/coin/transaction/tron	api_grpc.pb.go	ebe9b723f473755eca3dc5f04aaa9fecca717c60d5edffe17de3bd2654bbc12e
Wallet-Core/coin/transaction/tron	asset_issue_contract.pb.go	cb7038a37f3e09adbc00e0fecf4ae9104fcd855dafee93a6dfcd981f399f7115
Wallet-Core/coin/transaction/tron	balance_contract.pb.go	9a16e3a581ad33cc109305440e94ff2c1e5c0bc85aa8c0cfee54b1575f2a9bd5
Wallet-Core/coin/transaction/tron	common.pb.go	0c596820266b49d5e22a86bf632e97b435ea75829bdd9d2f11c19f0867f04e6d
Wallet-Core/coin/transaction/tron	exchange_contract.pb.go	b7eeb218611a8841d0ada9a42be342a117dc08a927bd57b7444acb58bf492310
Wallet-Core/coin/transaction/tron	market_contract.pb.go	7cfa0fde5e7195f088d6216f4671157b5f5f116eec64e3b396c17abdacc86f78

ID	文件	SHA-256 checksum
Wallet-Core/coin/transaction/tron	proposal_contract.pb.go	54209e3d5dc942bbaf1aacea0653253df460b200972a3be0a2ef923b1252a4f6
Wallet-Core/coin/transaction/tron	shield_contract.pb.go	0aa947ab7d006b4c315704d7318c80cf01a8e76e9218f192a58806d2c5136b75
Wallet-Core/coin/transaction/tron	smart_contract.pb.go	33014e47b1dd029e3e3f481a48000e403af1308ceeef0f1f1abfd6bd519855be
Wallet-Core/coin/transaction/tron	storage_contract.pb.go	0bcbb0013eb8186404489609ecf71bc0e88f30deb12acd05f1ac6ba6d337f4a3
Wallet-Core/coin/transaction/tron	vote_asset_contract.pb.go	e6fda6ace39842f0e6a8c1f211261b5f4b94c1ebcc885aa9c7bfa75176ebdca7
Wallet-Core/coin/transaction/tron	witness_contract.pb.go	f9e328c5f24ec31a1451565fb5ed7a37c7de8629807affdca0be6e9c40da2fbc
Wallet-Core/coin/transaction	utxosign.go	658f136a163071323795fa95461f7d9ef374853241104360919cb6d34b9c3007
Wallet-Core/coin/transaction/zes	common.go	f516da2f326a41cd3fdcc2f4f4462bea51f8c15a0329d1f6c91a7535fcc00434
Wallet-Core/coin/transaction/zes	common_test.go	61b34a6a6325f43f537e970912ef625fc8761410b9682c0cba8d9d64e183f294
Wallet-Core/coin/transaction/zes	hash.go	315c0698dfb2779f8fb498c5376d11c0765baccecb237c26fc124bcb7cd77804
Wallet-Core/coin/transaction/zes	hashcache.go	a31870880c1adf54aa9c1b92a84b6b0a642dd37b631cda282d25b439514ae813
Wallet-Core/coin/transaction/zes	msgtx.go	46754cc48c47be52add0f7b4e419484e04694ede85d112f8dad30a02479b54a0
Wallet-Core/coin/transaction/zes	sign.go	98e6a9580d99c3273995b687152b33fa356ac0bb92fe3201ed3aa0ff1cbeb198
Wallet-Core/coin	tron.go	6d220298e8f35ce716c499b1c322f5236c54c800eee6c8c512d1bec746dbcae1
Wallet-Core/coin	tron_test.go	34c68448ef71ee272f4c4a1fa3566cc607f2e6f16bb7b3d3cbe030dac2bc88bb
Wallet-Core/coin	tron_token.go	5e5185788a6b4609e764e291947a40d03ee97ebf4813825a159d24becc78a3e3
Wallet-Core/coin	tron_token_test.go	b224a35e78424cb1bdbf7d8a3143185fb6e530adaa39926ff2115ab7037a2c7b
Wallet-Core/coin	usdt.go	fca9ef7187f0362069bf3f786845f4aafd4db848eceaf3e0eb89cf11aec9ba1c
Wallet-Core/coin	wallet.go	8bd4f61b50db747e0360239598a39f05a8cef7ac6609cd203356cf19fd491363
Wallet-Core/coin	waves.go	84a2280146be123de510e4524aba902fcb68853bcc2b4ad4479519a9f3945810
Wallet-Core/coin	zcash.go	787d4da9dd09a90c542df56763beda1889ba005e288b282bb6a33b4128ed8f51
Wallet-Core/coin	zen.go	964df6d8eca0b820aebf9ecd2df9f593116282704d5f7f06a917a10fd9fb3abc

ID	文件	SHA-256 checksum
Wallet-Core/core	core.go	92347dd2b4d9ec72f3664b412673ce24a8aa73518ac4439aefa58788cff42ace
Wallet-Core/core	core_test.go	433b96cbd6c62686c50fda1c4403e76c6bde8cab274409c2974beccbacc1c9dd
Wallet-Core/core	mnemonic.go	ae93cc9bf8cdcd8109ad41d9e67de54067b225a6572a159b67f0a13947ae5a22
Wallet-Core/core	wallet_manager.go	f6f47914e66875fac981bb2db415e636f613afd0b861c5e430c79e50af235ed3
Wallet-Core/core	wallet_manager_test.go	ce05a2e72dfb15275c4be1b135ea6a44aa6a0c202f3402874c7a41f9ec4ea535
Wallet-Core	go.mod	4a55fa04161614ccfd8a5959211a5d31ef97094b45557cb2db5b24b1d9df2eb0
Wallet-Core	go.sum	5dd458ce93dfcc62c3526f1d8afe323f1db4bc581ba4508dca88042c39e526a4
Wallet-Core	main.go	98c305faf94a2aea53a87467edc4249d476ac66761bcecb60e39ea3ee466d0c5
Wallet-Core/storage	common.go	96067da6fddd523bd5e69c7ddb40419ddca96e53ec2560e42bd16beb21028089
Wallet-Core/storage	const.go	bcd9068f4cc664c5f8c8dda0b0cb0a9efd4341d48933c55aeeb338e9154e38ca
Wallet-Core/storage	errors.go	80361fd7c7d5c68e0d936122bcfa7028ac789869db37c25ba9896291a00d3ccf
Wallet-Core/storage	tokenabi.go	0740f606801b83efc2d41be7d1245b29a368acea6cf35a507496d027ee3a0c77
Wallet-Core/storage	tx.go	52b6ed2b606837ebc30fc0a728a1b64043738314f3ced623fe2db4f82eeafa81
Wallet-Core/util	base58.go	e3112efa7a5012e2784d06a92a7ee1e34ea5b913f90d9606c78efff2dd9bc9a7
Wallet-Core/util/encoder	encoder.go	63b7021ce8abd266883cee5558aa23996164bc881fdb3b20fb07bfa95aec91b0
Wallet-Core/util	util.go	663e3703e526867512b2dc714f2179f5fc268c1738fee267b980c48d6757e4f4

3.4 Chrome

3.4.1 js-signlayer

ID	文件	SHA-256 checksum
packages/metax-signlayer	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-signlayer/tests	sol.test.ts	dead41f471e0ea562f7508fc465d0b9a20b2c53f877a4798c58f545797d4c3e3
packages/metax-signlayer/tests	bch.test.ts	0c459cac832c244aad767c1fc797ee58054c7dc4fcd64a7e3922b4fe97dc4501
packages/metax-signlayer/tests	ltc.test.ts	4d47cf702d2ed5783f71796188df441cad06eb4c73d20fa5e35ebdb326770c02
packages/metax-signlayer/tests	usdt.test.ts	7fe9ea35197900d8f971294317e6856faee569fa8790667ab5e29ed31b2121d7
packages/metax-signlayer/tests	trx.test.ts	693ca713099dde2919596b4d69a1ee938239417236a9e9e41da7a865ba04cd6b
packages/metax-signlayer/tests	eth.test.ts	d67c095396da2bedbb09043b91c2c1ef0b14627ab51c5bcf1f199842aff81fa1
packages/metax-signlayer/tests	btc.test.ts	cef05c1e7ada35d6b02ed24b3f322e5223c42f19a42c12c0ed26a23b2ff68061
packages/metax-signlayer/tests	bsv.test.ts	d7aaed62f1ab363dc3b8ebee57d14128a054ba66a4f2335c76e20482b45e71a1
packages/metax-signlayer	package.json	12125f05f2e80c4dbd6ad3487a6563e40cf71963c0d777042f744e20bcee06ae
packages/metax-signlayer	tsconfig.json	d89d0f3ce0ed12faa875dd5d8caa1122d9c8d9078e5c70b7d50a9939d0cf7aef
packages/metax-signlayer/src	wallet.ts	f1018a45bcb7c2e8c634d90e5abd8388c1f6dd72c58c0911c20c4367719f87b9
packages/metax-signlayer/src	currency.ts	558ea371cbace51087c31d7fcefa38a9cd863d1bf6495715c553fa5f0e434d2d
packages/metax-signlayer/src	common.ts	a7805c464a093436d07d3c67d761db4312f4d7835476aa5c2a7f04b9753f3ad0
packages/metax-signlayer/src/basic	ed25519.ts	928ae1d457cd951a0a32d5f00b53d97c7a44f9c45aa97ae90ccfbdee25320196
packages/metax-signlayer/src/basic	typeUtils.ts	c456954444710ea0ca286abb5e38da7be634a45484b9ae2a0cb12e9475ad658f
packages/metax-signlayer/src/coins	SolWallet.ts	a436ca488bae682e31953681e23ae03381c2f526644d178ecd4215d3352fbdd8
packages/metax-signlayer/src/coins	EthWallet.ts	75631dfc8f3858e90f649c842a735e161e7764c5002612f3e267dbfdfdb0e42b
packages/metax-signlayer/src/coins	BtcWallet.ts	372f0a19db27a2a6422c52baa9a15f76a862e7c6f10ce5f84b2d78b50b81fdc2

ID	文件	SHA-256 checksum
packages/metax-signlayer/src/coins	TrxWallet.ts	fb43a9e45699a38719166453a4d997011d87ce20a5604751df27e9495250fc0e
packages/metax-signlayer/src/coins	index.ts	363e1808a209cb672792d37f42f0b4c6d084d3a78011736ddeb282c279cbd7b0
packages/metax-signlayer/src	api.ts	85e54cfe713076b2daa9731838a54610c42b8ef690cd086c526f7e91d490c8a2
packages/metax-signlayer/src	index.ts	43d54cfdb0d6a4e6e6fddedc218d6fa352ceea4a9af2cc2e802110614296402a
packages/metax-signlayer/src	error.ts	e899f7666b288552acac35c77c69c2247cf1799b08de0dbc26df8b78b38ac712
packages/metax-tron	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-tron/tests	trx.test.ts	09456a41dca41642cdfc94db1b2ca3da81a1bdfefab790504a6cf1b044ba8c4b
packages/metax-tron	package.json	50817ce285627b1fd0ebc9dccb2b645300469a86a79c0a171b2d2dc1a0fa5a67
packages/metax-tron	tsconfig.json	4811f4829954691be92b6d141fbb3d4a820d5001db3a3ff2f5e9850e2dab5359
packages/metax-tron/src	tronUtils.ts	196c7778003d9bf5bdd618a4596fb56c7578f428d17818b4e3c12ae92dbe2145
packages/metax-tron/src	index.ts	15eb36043911ff3e4dd4f05f59f4a2056e352b67356cc66b128e8a4dd158400e
packages/metax-tron/src/protobuf	Contract.proto	5987adb4793b3b99a5efb17d0a268300dc40cd436a0db837095c1aa91d42934b
packages/metax-tron/src/protobuf	tron.d.ts	5c390354e0fad3cabb3abdf11a947625161b7a29f534322388c35bb582333e07
packages/metax-tron/src/protobuf	Discover.proto	a1e1816ff6c5f3c8718e5e48044eff6ee9f974b1a258f00794d0ba100a0ede61
packages/metax-tron/src/protobuf	tron.proto	1b4c978460d0f2f5b5603734c90040cbd0dc27f67a3de7fc2a58151b41b1ade2
packages/metax-tron/src/protobuf	tron.js	ee37366f3273997f9ae8a65270450d07df45b27e42c7a5c8a656d85795670704
packages/metax-eos	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-eos/tests	eos.test.ts	0f0cf51b0cb3837ce33cbc41889c6edd05023a4cc34eb1837a47a281bfdf5e32
packages/metax-eos	package.json	bc2972667d77ed541fca6155392dcbae68f7b7c42327a7fcf77bdc96e9a0655e
packages/metax-eos	tsconfig.json	5e864c77545ffcd5993bb22254128e7dee90de4c47d4c9c084730336bed76971
packages/metax-eos/src	numeric.ts	ff795f96c2a9da21db4252300f12bcc16ce8f0b17c86db03c9caa48efb6380e2
packages/metax-eos/src	txBuilder.ts	bae13a25a87b973fbb821469484d22a547391271c2b1d142f33e66c93d466c04

ID	文件	SHA-256 checksum
packages/metax-eos/src	api.ts	9cadbd9ebccaeba082046eea371b601b5ac9a6d76142c86481f254c1ac454125
packages/metax-eos/src	action.ts	cf058b22383d24fab6afdf359641eeffd39a86ea2dad9501e31c97f7119aaf01
packages/metax-eos/src	types.ts	01964e2628fddb87534489e5904ed9e1d43d3d5c12c3be322edd071b47a4cca3
packages/metax-eos/src	index.ts	cb587e136c0289c873c07aff7823211efeaec2edd843182898eba4165c6278d3
packages/metax-eos/src	serialize.ts	d78e5ab155ab9cf29b3c3c1d6bef177b476cf5c6fae619defe79f6018bc71c32
packages/metax-flow	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-flow/tests	flow.test.ts	bbad3b9eb2a6a6df723d0b54dac916643d1f3ba3e52531a929070f359c8b0ad3
packages/metax-flow	package.json	78e9c4e47fe1ee1adba31b37c28f05a80d7c58b341c5a186d9d003e509aed306
packages/metax-flow	tsconfig.json	5e864c77545ffcd5993bb22254128e7dee90de4c47d4c9c084730336bed76971
packages/metax-flow/src	account.ts	091c105a5e42c3eb558ad87ddad20e433b5b9bdfd9931ccd3efd9ff8e55e17e2
packages/metax-flow/src	tx.ts	3b0f75f728def720ce0a5533ff88143e60b7f6a38c2c72ba94443825302e52e8
packages/metax-flow/src	signature.ts	39d8c2bf83e16667146d2e39c6c5a64366ab0e5c26ea35bfc33d595330d25eb1
packages/metax-flow/src	http.ts	7fac4a9fc1d31ea4b7135fb8f6b7445d44155c9cf3dbf8e75b11cfd8dfa48a9a
packages/metax-flow/src	model.ts	244c13016224237dbd362355c23be3a04d7dd33fee69e29ece853b1c624cf437
packages/metax-flow/src	enode.ts	120d7a1d8e57f373c7f78fcf3fc27cd4a0aadd2bc22d7686239aa6053bc9c82a
packages/metax-flow/src	index.ts	c71a50af6a497b81b7a677bc73fb5038be911c26f10c025a7a82de5cbacb9b7a
packages/metax-near/test	near.test.ts	ae648ed7df7c799542c029be068c65871af7814a7327fb554b2e1fa1e181f0f5
packages/metax-near	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-near	package.json	f7577e7189f386f24c193c599373db5cf6711764aef76e17ff70866fb363e027
packages/metax-near	tsconfig.json	94aff038b3e1ac65ddc7c63e323463b99aad966924ffdd143eca8f2447728367
packages/metax-near/src	keypair.ts	5e6454116ebca9e621f658d1ade1b39a234b8671d27d13544f4bfef16ce46f85
packages/metax-near/src	transaction.ts	f4bd6d36b1cad5b575318166529dc82957f50a2898344bee7f0104bfcbc21f98

ID	文件	SHA-256 checksum
packages/metax-near/src	index.ts	88f968b96f509aa5775b3bf6e44da3a5c7d31cca97b0d00f7c87cdaff77eacbb
packages/metax-near/src	enums.ts	d4edf55cdeb97fadeca3c6bb14783b3dd4fc1f3baf439fd0365548b402b459ba
packages/metax-near/src	serialize.ts	ea72941f6215d7a9d1fa929779175a2657e5f203808dc9bd505d2fc829ad0e66
packages/metax-solana	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-solana/tests	sol.test.ts	5be09507064748af8ee02fd13118f3fe99d91b891e24ae711a1bd7dfefdf1385
packages/metax-solana	package.json	a1d9b2e7fe545324bd2319e607080e8b280f1a7526816a45fccb15da5144b31e
packages/metax-solana	tsconfig.json	d89d0f3ce0ed12faa875dd5d8caa1122d9c8d9078e5c70b7d50a9939d0cf7aef
packages/metax-solana/src	api.ts	fe2beedae5e45a044d8044fff3ff9e64de323edb4b38f0df888d3d23bd02e0b7
packages/metax-solana/src/sdk/spl/instructions	transfer.ts	9d5384a017eec2112a8430fc51dbf41ef2cad7664c3b8543b59bfd36e0e8b82c
packages/metax-solana/src/sdk/spl/instructions	transferChecked.ts	229f8eebb5fd1087e99461addcb1fa355a385fec9dffeeec42b915576c6ec6de
packages/metax-solana/src/sdk/spl/instructions	associatedTokenAccount.ts	500dfc53a97b6f70ddf12e495497babfddcd3b146a57a7faf7e05c8c0db570ce
packages/metax-solana/src/sdk/spl/instructions	types.ts	e3f58883a242a8b533c010953d379efad95f955d7223092eea980db46fa4c3b1
packages/metax-solana/src/sdk/spl/instructions	index.ts	e083431012889bd6d0246eecf860165d62759d2880d0ae653375c7ca26830ef3
packages/metax-solana/src/sdk/spl/instructions	internal.ts	bf358147f2df7fc7539864cb6350c2ddf8816687d4a7182278463f5974220018
packages/metax-solana/src/sdk/spl	errors.ts	aa6981ce20561d80ce69d3943bf80842af73ae40660bbefcdd2c963beb5217f7
packages/metax-solana/src/sdk/spl	constants.ts	bc630c8d0863a016ff5ddc3db0ef4d5416753f5256e49d0d7015d95674ed86d9
packages/metax-solana/src/sdk/spl	index.ts	447c657f19211d69532c31fa5eae699a3a4f63a6db98c0c0bd1ae70298262ef6
packages/metax-solana/src/sdk/buffer-layout/utils	base.ts	b0fe4be45f6685487108f946aeaba92b1b197ffa21763fc00922eebdc037025f
packages/metax-solana/src/sdk/buffer-layout/utils	web3.ts	8dce1941fc154b0aecf16cb0e5cd0706ccc7c10bd916fd29db969aeb58cf9246
packages/metax-solana/src/sdk/buffer-layout/utils	native.ts	486e49ba6e68880661763406a62825b013581bbd6670f8aad6db67243c43bf6a

ID	文件	SHA-256 checksum
packages/metax-solana/src/sdk/buffer-layout/utils	decimal.ts	64b6938a4dd41de14baab8b320b213c4f3cbd351ee98ad13b613af5cca6338ee
packages/metax-solana/src/sdk/buffer-layout/utils	bigint.ts	7b6a88fb27446d2528832262384a4f22bbb67310d591f7d2a2192e2b628df3c4
packages/metax-solana/src/sdk/buffer-layout/utils	index.ts	cb8e78bad4cbf23406289a5ec14312e3abba608f21a7cc98a8c0ce6908ab1c4c
packages/metax-solana/src/sdk/buffer-layout	layout.ts	749e09480c072f61a300e097f6e2ccda58b20120f64e6979ce145140be90cb7e
packages/metax-solana/src/sdk/buffer-layout	index.ts	f53be365f764af493b13fd1daff50ea508b5715ac0add3a77fba762f8c45968c
packages/metax-solana/src/sdk/web3	instruction.ts	c397022a5d420cedf1c8e493cfa7007f0e1b0ea0c2e43cd60ba9ffb9795d58db
packages/metax-solana/src/sdk/web3/util	to-buffer.ts	a3d6e55f43facd349cf4b5597a33ea06d0c81f5ebe1bbc6d0810808494f6c75d
packages/metax-solana/src/sdk/web3/util	shortvec-encoding.ts	b8c2649037607b056f9dac8e4888898d5319941545f994924ceb934d562870a7
packages/metax-solana/src/sdk/web3/util	borsh-schema.ts	c9fd047494d1643e1e04d659b23a3d536050f348e648f37168796cbe3c3e548c
packages/metax-solana/src/sdk/web3/util	sleep.ts	bfef80704d32763bd89639edd51fcc71f2c27d5002feb5420d47173518f03bcc
packages/metax-solana/src/sdk/web3/util	tx-expiry-custom-errors.ts	d2a920d5464d490f6aeea4e811046e9edb86585012cb2dc5f64363e5bd5c225b
packages/metax-solana/src/sdk/web3/util	cluster.ts	b2529331489a93d5aaabfb4abe0ccba37f090209e17ddc0d656a85007716bd0f
packages/metax-solana/src/sdk/web3/util	url.ts	52bf396152d98e55802025c40dddff1b005b390ded59065e98dea27ffe223e41
packages/metax-solana/src/sdk/web3/util	assert.ts	60e5ab3b96de03c3160b963a79fdfbe5bcc08b52e795e7f805699c74eac5f364
packages/metax-solana/src/sdk/web3/util	bigint.ts	dd466f10a1e88acbf84ec2d6d9318ac895957350e3fdf88970505a4d021b9ee9
packages/metax-solana/src/sdk/web3/util	promise-timeout.ts	9a06d7fb9a02ee337c4f4fef7c9431e768f7d903384dc0e3cd30b9b7b71bd331
packages/metax-solana/src/sdk/web3	publickey.ts	0a72de29b65c50331333ace1545a9c07a99e24a8bdf6b64ce78ed7f970603612
packages/metax-solana/src/sdk/web3	blockhash.ts	efffb098704ef16b532391713e19e85609e6cfe6550f10e98694391f89cc76b5
packages/metax-solana/src/sdk/web3	keypair.ts	af9389f2a9bc0f1ad5c28d76125884137d622343278973f5a0b15fa1349ad2f7
packages/metax-solana/src/sdk/web3	nonce-account.ts	3eeeee497b664814f33635e4f46df3a6306e126da7336999e54a9107cbd474f1

ID	文件	SHA-256 checksum
packages/metax-solana/src/sdk/web3	fee-calculator.ts	5ecad0bc24debe79a37e6efe9ddc11117093791d63bba37961c59aec9526bf8f
packages/metax-solana/src/sdk/web3	system-program.ts	5c071b0d32e45662eaacdfb8245b824d9d278e4f9e806de6f586e55e13f7d47a
packages/metax-solana/src/sdk/web3	message.ts	4f62b88c3efb57a0c6beb46e1a610e398c03301282a53c47083a8d321ed11f37
packages/metax-solana/src/sdk/web3	transaction-constants.ts	3b836583bf21e1877cd8c0733c68167c8c3b42714941a216db78239599c5c677
packages/metax-solana/src/sdk/web3	layout.ts	9c1a7d71689beeb4966c40d413a22c8bab8ea681916aa0d3496c592afaf08100
packages/metax-solana/src/sdk/web3	stake-program.ts	c31fbf192f078c07142fdf509ac1feba2f60274f67020a1f9b85a4a729020f59
packages/metax-solana/src/sdk/web3	transaction.ts	a45d1043be10949c5e42d867136e8d373d9784b1da816c600614aedbfea034c8
packages/metax-solana/src/sdk/web3	index.ts	f60e2c65734915bec19e14016b69ac137f3d370ea38fa9a1cd2e1d63ce543fce
packages/metax-solana/src/sdk/web3	sysvar.ts	2b0ef75268de86a90b8c2b8bad7c7cf5a3167ac876b2daef25daa289bce227d0
packages/metax-solana/src/sdk	index.ts	1a9990dabf9e78f0733b9229ae3f0bba3260c3a117db0498a0df8f09ce784a5a
packages/metax-solana/src	index.ts	9b12e7fe7d4aec8b8a29e9804a35cf998baf37e2faaa307fa96c1bd2cc80da15d
packages/metax-cosmos	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-cosmos/tests	luna.test.ts	6714d9c58539f373c5c49425fb2778cdb2a16d5b58fd7720fb3a6fe4e2a41f9f
packages/metax-cosmos	package.json	6b042d928359b707fbc385fd6697fa861ae133c438a62e936b535bc7f9890777
packages/metax-cosmos	tsconfig.json	4811f4829954691be92b6d141fbb3d4a820d5001db3a3ff2f5e9850e2dab5359
packages/metax-cosmos/src	tx.ts	c4dbe6c3dc559da9b6b472d2fcbd6ab228f6523efef4c32fc01661014ff88366
packages/metax-cosmos/src/types/gogoproto	gogo.ts	4317d7a35fb3ae468a4965111e4312e1db2b3c63583d055697fcebbcd446b06b
packages/metax-cosmos/src/types/google/api	annotations.ts	b158d65d082fa3993f0102bd696389d25f5b1b0885be46622113cd9cd8337bab
packages/metax-cosmos/src/types/google/api	http.ts	08e8b5d71259695cf09d9d6c78f874c1dde0a3b41afbe8f6c580281c2ffe5029
packages/metax-cosmos/src/types/google/protobuf	any.ts	9badfbda6c0f6196d8b0954c6f2ac62693b531d400021d5980279bd8d8077ed5

ID	文件	SHA-256 checksum
packages/metax-cosmos/src/types/google/protobuf	timestamp.ts	f07560bb1b992268fd1a72e4f09692efce2083fe4bd0b7951ed765aa62ce87af
packages/metax-cosmos/src/types/google/protobuf	duration.ts	07927c6a00c5499c6e5629a752d06a034ee6968230c3638009cbacc4a9888537
packages/metax-cosmos/src/types/google/protobuf	descriptor.ts	f78d5479041db15bc8d853bdd43151b428324886faf464596de59737354b3b21
packages/metax-cosmos/src/types/cosmos/crypto/	keys.ts	e1482863ca3fd6498a2c6085085963 7f6882b1034b978837ac03fcbda13bb5a8
packages/metax-cosmos/src/types/cosmos/crypto/	multisig.ts	f884a337eb683a112d9333ad3a57188abd36eab7374228d2311c53e427eae985
packages/metax-cosmos/src/types/cosmos/crypto/	keys.ts	dd6f01c2ed48fcbe50407ddc979600e52ee9f040c5cd6b1854b60c0f0e658b1c
packages/metax-cosmos/src/types/cosmos/crypto/	keys.ts	d2608f47140c7e93bb90c4bbcdf5f9499dc3abc8de1d55016855d8a3d2fa8733
packages/metax-cosmos/src/types/cosmos/bank/v1beta1	tx.ts	99f69ee951d9eb7dc4fb31a2a11fd36aa9f74cdb994bf08eba3b228ea365297e
packages/metax-cosmos/src/types/cosmos/tx/signing/	signing.ts	8fa56c102c9b58fdd6e30938e040bff98275847d216681b58a778ddcbb63aa68
packages/metax-cosmos/src/types/cosmos/tx/v1beta1	tx.ts	bb771d64f2b8bb905eb63e6f90d1e47ab4228ebe4ba01b2fc9e1b1688646826d
packages/metax-cosmos/src/types/cosmos/staking/	tx.ts	db6b10d1403e7cf6271b5f962b2a2ea35475bd5f24d1c06dc84d5d1f1e0b8d12
packages/metax-cosmos/src/types/cosmos/base/v1beta1	coin.ts	6a42a1a7f0bf7ce16bb45ca1142f970587108908dca3ec8df2722043f4535c2b
packages/metax-cosmos/src/types/ibc/applications/transfer/	tx.ts	1c81ac8d9fe7ca73d99ad07f336f67cebc5ad8104456d7a9b1c3cec5c0a1027d
packages/metax-cosmos/src/types/ibc/applications/transfer/	transfer.ts	f47953a8e8a8aaead9433364d4a613476f76153cc47b4b75b70a7e8961f257ba
packages/metax-cosmos/src/types/ibc/applications/transfer/	packet.ts	0c710e1655c653251cabff2150ddaa6b06bc8f00050d3d1491bf0028b1b1b35c
packages/metax-cosmos/src/utils	array.ts	eba9b96efc7abbdff5a4c4713dd316a21f8d1744dcd959e7c0709779bb8a68a3
packages/metax-cosmos/src/osmosis	aminotypes.ts	08a532c9a69b6dbbddadf40f0187c254ee0a32c0a652381f532fbdab294d4c07
packages/metax-cosmos/src/osmosis/gamm/v1beta1	tx.ts	231b7939dc7b54a863b98a5b934a1aa212ac4db596f268fcfb60083b23b8baeb
packages/metax-cosmos/src/osmosis	registry.ts	d083468cfef1908fd6fab3ed15cbbaf0a0736656f15a95a5fa683e4db3988bea
packages/metax-cosmos/src/osmosis	index.ts	af4f9ae563861c4bcbae68bfb218314f2c30c71c840bbbd7cdc988c2c229665e

ID	文件	SHA-256 checksum
packages/metax-cosmos/src/amino	aminotypes.ts	13beaed418fe44df9d3a166f04e1654ca58a6a29bcf85149447bad0687ffc419
packages/metax-cosmos/src/amino	coins.ts	5055c7987873873f450eb6124f43962908f542e9737a41aa419c84a11cb0bdd4
packages/metax-cosmos/src/amino	pubkeys.ts	6f262c588aa6c5ee11565bb2144dc0213eb1927096d47966acbb6739c3e22039
packages/metax-cosmos/src/amino	encoding.ts	587ad6ca64759eab6f2fcc096ddc310631bfb6407fda4b1f35ecf841470badb9
packages/metax-cosmos/src/amino	aminoRegistry.ts	12a1c4a80ae45791c018da300a7591f51a40c51f8a3c9636d72815f59a1c523e
packages/metax-cosmos/src	registry.ts	3325f6781457dc7bb58b6c6913d2c5a23a9374cfd0ad2ca59b47e263d945855f
packages/metax-cosmos/src	index.ts	a15e7352419a2b421e1de5f047f1205af782f299ff308a6f17280d606fbf09ba
packages/metax-cosmos/src	encoding.ts	1f1a3c6c39a4ba7f1ac192df1f8f051a95730a57a28d49fb918abb303a3cdafc
packages/metax-ethereum	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-ethereum/tests	eth.test.ts	603653c7ac6eedcdb067eb5e64dce6c6405a7147d610e5748a224f2930076e92
packages/metax-ethereum	package.json	71e63f93fd8ea8bbe3916f554d75f4b4b708590b6a0537310c166174fb9be52b
packages/metax-ethereum	tsconfig.json	5e864c77545ffcd5993bb22254128e7dee90de4c47d4c9c084730336bed76971
packages/metax-ethereum/src	api.ts	9176a722f96d9d7689094f39c715dc984c9bd7830d0a2d824fe9db9103dae1fc
packages/metax-ethereum/src	message.ts	e218f65ddc3164d1af5eb6d89ec4292fa694e84378463f3061422906ca94b97e
packages/metax-ethereum/src/sdk/ethereumjs-tx	baseTransaction.ts	c5a4351973677e0e106f873f22a701a5659278ba3a618b3759dbc572a2cb2bb9
packages/metax-ethereum/src/sdk/ethereumjs-tx	legacyTransaction.ts	ba169238caad5aabbbcf1a8c3e8d1187d71ddfa8af02f97f00d4d23f93e3be5c
packages/metax-ethereum/src/sdk/ethereumjs-tx	types.ts	0b8935f19781558459cb78f4387a82e5805722d51888a277bd657b4f176fa51e
packages/metax-ethereum/src/sdk/ethereumjs-tx	eip2930Transaction.ts	77a25c583fb7e7da287bf484f33146f4cb37b3da995c57d25678b4fe81674af4
packages/metax-ethereum/src/sdk/ethereumjs-tx	eip1559Transaction.ts	34b100c9aa61bf5a7e157902d50edfaf0e6d488a7eb1d9aff8b0c0d7f5b1ed55
packages/metax-ethereum/src/sdk/ethereumjs-tx	transactionFactory.ts	ab233d3b947ea5480fd749347484ead8fdc94247b79352cce58c354110baac8f

ID	文件	SHA-256 checksum
packages/metax-ethereum/src/sdk/ethereumjs-tx	util.ts	ce4001efe2ac98c5b8cc6a55e6b2014369eb6dd5f10eac728ceec0c4018e76f2
packages/metax-ethereum/src/sdk/ethereumjs-tx	index.ts	3eb43bcb37b9d93ff5c6b8a5927605dac6c6b517e67f45eff19556fa35d4921c
packages/metax-ethereum/src/sdk/ethereumjs-util	account.ts	048e3fd0ac4b9d55e23c5e2eefffb11b315642c90463a33bcf642eae7e316bc8
packages/metax-ethereum/src/sdk/ethereumjs-util	helpers.ts	c190716558127868b09cef6231c4f4e6366d36763cfca0c7e63dd829b02406c6
packages/metax-ethereum/src/sdk/ethereumjs-util	signature.ts	6a9c6d6e058ab7977ebdd754fc8a50584c2bea82c65c9537e59f9db49bfc8181
packages/metax-ethereum/src/sdk/ethereumjs-util	bytes.ts	354e4eedbf8f0b003dd593e236b372a873998a55297de3a6a61f7d3e657908b9
packages/metax-ethereum/src/sdk/ethereumjs-util	hash.ts	50ff1b736776cea4acb19b7bd7f1c0abe1175b99461ef29abcd558f4edc5e00f
packages/metax-ethereum/src/sdk/ethereumjs-util	types.ts	dcb0cf9114b439b2351b230290af7a31b92a22425c55dbe52f29c953877e5584
packages/metax-ethereum/src/sdk/ethereumjs-util	constants.ts	decea0f5c3735dde2c1ac242c0167f3f45d9ada533a5cd6ff74d8778a0896666
packages/metax-ethereum/src/sdk/ethereumjs-util	util.ts	396d185582726c582585a4b1a54fe1d8e38ccc465b83670e7288892676ecbaaf
packages/metax-ethereum/src/sdk/ethereumjs-util	index.ts	f74cb4f6ca749070402192c970b15febf0b10e4090c7a5a0248e8148c17f0f0c
packages/metax-ethereum/src/sdk/ethereumjs-util	rlp.ts	722c6a95f6293d455c04582bdddd7f4d265270179dfdce61bd498dae4515a83f
packages/metax-ethereum/src/sdk/ethereumjs-util	externals.d.ts	492e93d4239e5ee0a7a39d927059558f128dea54ee4d4c0b8e6e2f4f063537f9
packages/metax-ethereum/src/sdk/ethereumjs-util	address.ts	8a3e119a979c24c442bc94dc076daf52b70e0d604b4b29fba96972acd2323920
packages/metax-ethereum/src/sdk	index.ts	9d8b820bddd0d40c9ab00c6c301fd1204aeae7a290c666bee5eef44c4064d486
packages/metax-ethereum/src/sdk/eth-sig-util	utils.ts	7d7ca8831bfd2e4248fec30d699244d0ca030765332616438e72d7739abc6381
packages/metax-ethereum/src/sdk/eth-sig-util	index.ts	11e929d05ba03a70feb28a68328503bbf642a241da42c99dc74af2f3adb478f4
packages/metax-ethereum/src/sdk/eth-sig-util	sign-typed-data.ts	b445e6d01ef1a118283c0852c0224ec51023c4309e677c6b7a3cfafdac8793dd
packages/metax-ethereum/src	index.ts	6093ed0db1e0da30824a4b573ab20c878a6aa857d85272dda47e53530b687e38
packages/metax-bitcoin	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754

ID	文件	SHA-256 checksum
packages/metax-bitcoin/tests	btc.test.ts	4066f1e597d5f4b1d22cb03e8729ba020066f7c19c0361e2952cd58706bba369
packages/metax-bitcoin	package.json	fbce6a4f623164e0367e1380b6c9a16b8aca61aff66ef889c9d43900a1603744
packages/metax-bitcoin	tsconfig.json	4811f4829954691be92b6d141fbb3d4a820d5001db3a3ff2f5e9850e2dab5359
packages/metax-bitcoin/src	wif.ts	46002aa65160674e0d697a9d235a70dd71ad8f2f5d8c0aa23c453be6388c9b65
packages/metax-bitcoin/src/bitcoinjs-lib/payments	lazy.ts	bdc7e905977992be0599f0ebed3af59ef75b8cb55cd635e3c5babbad4f857d9e
packages/metax-bitcoin/src/bitcoinjs-lib/payments	p2pk.ts	d2b1dbd31eaa3591b439ad52d9940bb14e4ece4110880162a7f033d817c456fd
packages/metax-bitcoin/src/bitcoinjs-lib/payments	p2wpkh.ts	426851c59daaad711f2690639669bab9497a70fe39a6866bb34eac1695b3bbb8
packages/metax-bitcoin/src/bitcoinjs-lib/payments	p2pkh.ts	d1db9ae4737369bde92624f98351ec9feb577c672a014679dae770c8fa25846f
packages/metax-bitcoin/src/bitcoinjs-lib/payments	p2ms.ts	663e384e180b61c525021e020ddf340385fe36f95a16f0526a3245c8284ef13d
packages/metax-bitcoin/src/bitcoinjs-lib/payments	p2sh.ts	468e59160830ebfd3bb2fae8ffd15b6c3a71671266f96aef9744a2e777df4259
packages/metax-bitcoin/src/bitcoinjs-lib/payments	index.ts	62842483c3e1e336418fd93f0af22a225b2fa1c60ace5c2a9d9fe95aa1671308
packages/metax-bitcoin/src/bitcoinjs-lib/payments	embed.ts	3e7318c6615b8a28fb6e501f43703a03d67e82b7b66d7283c5e7fa053bcb4550
packages/metax-bitcoin/src/bitcoinjs-lib/payments	p2wsh.ts	f6f7d6cc2f6e90e5154a2cb8933123dd611c1f21addcdcef865b098d75f889b0
packages/metax-bitcoin/src/bitcoinjs-lib	script.ts	7427e483f4b677ebd78fe0e32439a671c97d9530ff37527c09ae36822203f6ae
packages/metax-bitcoin/src/bitcoinjs-lib	bip66.ts	f16e696f585e666780b231c4c4867058003b139685dfca23d0db49ab9a96b662
packages/metax-bitcoin/src/bitcoinjs-lib	varuint.js	72df5247058acec046656e3c99f0e990a1e6730b9a28bc7422399b52f184f2df
packages/metax-bitcoin/src/bitcoinjs-lib	push_data.ts	8922ab7ce6652216662aea466bdb7c71c488b6a1dcd036b2461f45db5fec78a0
packages/metax-bitcoin/src/bitcoinjs-lib	bufferutils.ts	dcb8aa011aadea926ff3980a9f23ebb06116454bc5f13572b5c27d20c0380b52
packages/metax-bitcoin/src/bitcoinjs-lib	crypto.ts	568d2787a196f1949351fa250ba5c13769525e7d338c6a551d16ab72ed8e84ab
packages/metax-bitcoin/src/bitcoinjs-lib	ops.ts	e7a1979bd0e8604402c7e3f7572bfe83acb0e800fb3cb274ef6b02964a725ee5

ID	文件	SHA-256 checksum
packages/metax-bitcoin/src/bitcoinjs-lib	networks.ts	4f353a8203784f34ef2b93ae1588fac5e07dcbd469df17a6dbffe8947b60a03a
packages/metax-bitcoin/src/bitcoinjs-lib	types.ts	51fe18071b1f8c0f030b55dd8b36b36946e566cf5b104cb3170f2188f46a9cec
packages/metax-bitcoin/src/bitcoinjs-lib	script_signature.ts	13bf22bb32d72750c5353a9b211a8c8ea098facf48e8ba3956d9073e68538e9d
packages/metax-bitcoin/src/bitcoinjs-lib	varuint.d.ts	3b2119df3d7142228be799e6ea896c797ff796cf51ea8272a5fd503cbc4b7dfd
packages/metax-bitcoin/src/bitcoinjs-lib	transaction.ts	1ffb1b95837ff30a8d96d800ee0868a53cd84128fd6a353dffd829a5bcee9669
packages/metax-bitcoin/src/bitcoinjs-lib	index.ts	c766a97b9f0d473530acbfa0d1e804fed561ae860e082cda8936bbcaa07a6317
packages/metax-bitcoin/src/bitcoinjs-lib	script_number.ts	cc15c1fe9cf88200c8d06f1624b35ff209ff374d55aaa0f7926daee3f854799f
packages/metax-bitcoin/src/bitcoinjs-lib	address.ts	8871b9b65346cdf196d0f6710ac5573a7388d57fc6c885e82c0fa0706ef6c7e3
packages/metax-bitcoin/src	txBuild.ts	91cd5db8c7b94dadf3542345f98eed68d7308cd13277d0b1c5f796b975c8c385
packages/metax-bitcoin/src	type.ts	7ca533c8030e971603ab68ae95bbabc2c75b9d3b3a8d4842222d6bf226b5b5d1
packages/metax-bitcoin/src	index.ts	29a27c3167a7b0b425ae50d0a4120a6d3ab550c3b570ec66a4504a53de208134
packages/metax-crypto	jest.config.js	6a16b4064c3f23792c832a1621385df64f6b63eb4dd93251d7d600ab52272754
packages/metax-crypto/tests	batch.test.ts	b0c7fe99c5cf536f2fe965333e72eeeeb46004a6b6cc35199fa47f75bf037e13

3.4.2 keyrings

ID	文件	SHA-256 checksum
	KeyringController.js	401aebf92d493d391fe5c86f1f7d524be3f1ca9d60618ecddd0f237b3c63c511
	keyringUtils.js	c27a6aac576b4cdec0bb29cba6da4260d2147930307a60435f9e4c497e43e86c
	MultipleTrezorKeyring.js	c0f220457532dac941428149280025384 6d35ed6ed30cea3bb1b48ef3e4552d5
utils	index.js	f0fd99e30b3034a9988d897ca3453002bd16b9d9e8f3fdc259b22859b30e1ce0
utils	transfer.test.js	e3e57f74bbb8126a61e3bf48f594d35ea33675731b7119460018acfc02eceba7
utils	transfer.js	409941f93384010fd89c285863be10bcccae945b722e7443d20363da9925105f
	MultipleSimpleKeyring.js	5bcb68852e21c090905a9a69beeca165e4b5c1acc72855baaec073f52c5974ac
	MultipleHDKeyring.js	0933e34c151095afabb5ad19ff1a99d47b31d66d7b750cd9f6bb27e684e311f8
	MultipleTrezorKeyring.test.js	68d94a4fdd1073b435e2785065d9381f176f0b5424332f970e639bf3d3755e4a
	MultipleKeyring.md	27b726506c46b5b60d6534bb9edbba164968bc1e0ea5ffa52ae350547cd88908
	KeyringController.test.js	22b64a1a5ca85f5aebc157a08528f95ce98a28202855a86cf7770e912a5780a2
	MultipleHDKeyring.test.js	4bbec2bfad8a5507ba77e7f14e035855ccd0a0c2c3b2ccc88a6df9a427e40d84
	MultipleLedgerBridgeKeyring.test.js	da0e0dfa1e741b11d673dc7cc47bdae4a47513e6f254bbef8fb0d92278fc4062
	MultipleSimpleKeyring.test.js	0df5a610ac67d59b5740a2fbd842f81c395f1af047e5fb3df81a8eb22f4dc3b3
chains	index.js	9317db3d5f64c6c4488949ae5931bd23aeae866e5767b43702b109e3d8074e8b
chains/ethereum	SimpleKeyring.test.js	84f5f5968a93d379c6eb418ce0f6dec496110eb9e038d8cc1465dcadfec3b173
chains/ethereum	HDKeyring.js	b32739718e2788595f2bda9986e3facdcf0d4855221d7666c487304d8ba90c39
chains/ethereum	SimpleKeyring.js	66b84f09bbafb1a4e94aa0d84282099951db70454cd248403f4d49e88b5bdacb
chains/ethereum	HDKeyring.test.js	77aedcee7185840e211c154cd9b8f540870674a7a0077235c2c985cd45db1d40
	keyringUtils.test.js	1d49ae40330043dd672c6c2e95864be2cac14cddaaaee8c302e3a2109671aae4
	MultipleLedgerBridgeKeyring.js	0b119601997af6885425c956a15c344eecb9ef16c2acb808c8159b5660a977e0

4. 代碼結構

4.1 Android

```
├── IWalletManager.kt
├── PasswordManager.kt
├── WalletApiService.kt
├── WalletBridge.kt
├── WalletBuilder.kt
├── WalletCreateUtils.kt
├── WalletGenerator.kt
├── WalletImpl.kt
├── WalletLoader.kt
├── WalletManager.kt
├── database
|   ├── WalletDatabase.kt
|   ├── address_book
|   |   ├── WalletAddressBookDatabase.kt
|   |   ├── WalletAddressBookManager.kt
|   |   ├── WalletSendCoinRecordManager.kt
|   |   ├── dao
|   |   |   ├── AddressBookDao.kt
|   |   |   └── SendCoinRecordDao.kt
|   |   ├── entity
|   |   |   ├── AddressBookEntity.kt
|   |   |   └── SendCoinRecordEntity.kt
|   |   └── repository
|   |   ├── IWalletAddressBookRepository.kt
|   |   ├── IWalletSendCoinRecordRepository.kt
|   |   ├── WalletAddressBookRepository.kt
|   |   └── WalletSendCoinRecordRepository.kt
|   ├── dao
|   |   ├── AddressDao.kt
|   |   ├── DAppDao.kt
|   |   ├── KVDao.kt
|   |   ├── MessageDao.kt
|   |   ├── SyncDao.kt
|   |   ├── TxLogDao.kt
|   |   └── WalletDao.kt
```

```
|   ├── entity
|   |   ├── AddressEntity.kt
|   |   ├── ChainAddressEntity.kt
|   |   ├── ChainAddressSegWitEntity.kt
|   |   ├── DAppFavoriteEntity.kt
|   |   ├── DAppHistoryEntity.kt
|   |   ├── DAppSearchHistoryEntity.kt
|   |   ├── DAppTabEntity.kt
|   |   ├── EOSInfoEntity.kt
|   |   ├── KVEntity.kt
|   |   ├── MessageItemEntity.kt
|   |   ├── RootWalletEntity.kt
|   |   ├── SepInfoEntity.kt
|   |   ├── SyncItemEntity.kt
|   |   ├── TxLogEntity.kt
|   |   ├── WalletClosedCoinEntity.kt
|   |   ├── WalletCoinEntity.kt
|   |   ├── WalletDefiEntity.kt
|   |   ├── WalletEntity.kt
|   |   ├── WalletNftEntity.kt
|   |   └── WalletOpenedCoinEntity.kt
|   ├── migration
|   |   ├── FlutterWalletDBHelper.kt
|   |   ├── IMigration.kt
|   |   ├── TableAddressMigration.kt
|   |   ├── TableChainAddressMigration.kt
|   |   ├── TableCoinMigration.kt
|   |   ├── TableEOSInfoMigration.kt
|   |   ├── TableKeyValuesMigration.kt
|   |   ├── TableMessageMigration.kt
|   |   ├── TableSepInfoMigration.kt
|   |   ├── TableSyncMigration.kt
|   |   ├── TableWalletMigration.kt
|   |   └── WalletDBMigrationWorker.kt
|   ├── repository
|   |   ├── AddressRepository.kt
|   |   ├── DAppRepository.kt
|   |   ├── IRepository.kt
|   |   ├── KVRepository.kt
|   |   ├── MessageRepository.kt
|   |   ├── SyncRepository.kt
|   |   └── WalletRepository.kt
```

```
|   ├── utils
|   |   └── WalletSQLiteOpenHelper.kt
|   └── view
|   ├── ClosedCoinView.kt
|   ├── JoindChainAddressView.kt
|   ├── JoindCoinView.kt
|   ├── JoindDefiView.kt
|   ├── JoindSepInfosView.kt
|   ├── JoinedChainSegWitAddressView.kt
|   ├── JoinedNftView.kt
|   ├── OpenedCoinView.kt
|   ├── RootWalletView.kt
|   └── WalletView.kt
├── interaction
|   ├── DappBaseInteraction.kt
|   ├── DappBaseSignInteraction.kt
|   ├── DappInteractionFactory.kt
|   ├── bean
|   |   ├── DappInteractionFeeInfo.kt
|   |   ├── DappInteractionResult.kt
|   |   ├── DappSignInfo.kt
|   |   └── DappTxResultBean.kt
|   └── impl
|   ├── EvmDappInteraction.kt
|   ├── EvmDappSignInteraction.kt
|   ├── SolDappInteraction.kt
|   ├── SolDappSignInteraction.kt
|   ├── TrxDappInteraction.kt
|   └── TrxDappSignInteraction.kt
└── transaction
├── OKWTransaction.kt
├── TransactionFeeInfo.kt
├── calculator
|   └── OkCurrencyCalculator.kt
└── impl
├── OkAccountTransaction.kt
├── OkCosmosTransaction.kt
├── OkEosTransaction.kt
├── OkNearTransaction.kt
├── OkPolkadotTransaction.kt
├── OkSolanaTransaction.kt
├── OkTronTransaction.kt
├── OkUTXOTransaction.kt
└── OkWavesTransaction.kt
```

4.2 IOS

```
├── AFNetworking-4.0.1
|   ├── AFCompatibilityMacros.h
|   ├── AFHTTPSessionManager.h
|   ├── AFHTTPSessionManager.m
|   ├── AFNetworkReachabilityManager.h
|   ├── AFNetworkReachabilityManager.m
|   ├── AFNetworking.h
|   ├── AFSecurityPolicy.h
|   ├── AFSecurityPolicy.m
|   ├── AFURLRequestSerialization.h
|   ├── AFURLRequestSerialization.m
|   ├── AFURLResponseSerialization.h
|   ├── AFURLResponseSerialization.m
|   ├── AFURLSessionManager.h
|   └── AFURLSessionManager.m
├── OKBAsyncLoader.h
├── OKBAsyncLoader.m
├── OKFAPIBaseManager.h
├── OKFAPIBaseManager.m
├── OKFAPIURLRequest.h
├── OKFAPIURLRequest.m
├── OKFAPIURLResponse.h
├── OKFAPIURLResponse.m
├── OKFCachePolicy.h
├── OKFRequest+Private.h
├── OKFRequest.h
├── OKFRequest.m
├── OKWApiService.h
├── OKWApiService.m
├── OKWBridge.h
├── OKWBridge.m
├── OKWDataBaseManager.h
├── OKWDataBaseManager.m
├── OKWMnemonic.h
├── OKWMnemonic.m
├── OKWSchema.h
├── OKWSchema.m
├── OKWWalletManager.h
└── OKWWalletManager.m
```

4.3 Wallet-Core

```
├── build
|   ├── gomobile
|   ├── index.go
|   ├── index_test.go
|   ├── makefile
|   ├── nft.go
|   ├── patch_286.go
|   └── test
|   ├── base_test.go
|   ├── cosmos_test.go
|   ├── elrond_test.go
|   ├── eos_test.go
|   ├── harmony_test.go
|   ├── near_test.go
|   ├── okt_test.go
|   ├── polkadot_test.go
|   ├── solana_test.go
|   ├── starknet_test.go
|   └── tezos_test.go
├── coin
|   ├── achain.go
|   ├── achain_test.go
|   ├── ark.go
|   ├── ark_test.go
|   ├── bitcoin.go
|   ├── bitcoincash.go
|   ├── bitcoincash_test.go
|   ├── bitcoingold.go
|   ├── bitcointest.go
|   ├── bsc.go
|   ├── bsc_test.go
|   ├── bsc_token.go
|   ├── bsc_token_test.go
|   ├── cosmos.go
|   ├── ctxc.go
|   ├── ctxc_test.go
|   ├── dash.go
|   ├── digibyte.go
```

```
|   ├── elrond.go
|   ├── eos.go
|   ├── eos_test.go
|   ├── etc.go
|   ├── etc_test.go
|   ├── eth.go
|   ├── eth_test.go
|   ├── eth_token.go
|   ├── eth_token_test.go
|   ├── evm.go
|   ├── evm_token.go
|   ├── evmos.go
|   ├── flow.go
|   ├── harmony.go
|   ├── icx.go
|   ├── icx_test.go
|   ├── litecoin.go
|   ├── nas.go
|   ├── nas_test.go
|   ├── near.go
|   ├── neo.go
|   ├── okp.go
|   ├── okp_test.go
|   ├── okt.go
|   ├── okt_test.go
|   ├── okt_token.go
|   ├── ont.go
|   ├── polkadot.go
|   ├── polygon.go
|   ├── polygon_token.go
|   ├── qtum.go
|   ├── qtum_token.go
|   ├── ronin.go
|   ├── ronin_token.go
|   ├── sign
|   |   ├── dot.go
|   |   ├── eip712.go
|   |   ├── eth.go
|   |   ├── op.go
|   |   └── tron.go
```

```
|   ├── solana.go
|   ├── solana_test.go
|   ├── starknet.go
|   ├── starknet_const.go
|   ├── tezos.go
|   ├── transaction
|   |   ├── act
|   |   |   ├── act_tx.go
|   |   |   ├── act_tx_test.go
|   |   |   ├── condition.go
|   |   |   ├── condition_test.go
|   |   |   ├── encoder.go
|   |   |   └── encoder_test.go
|   |   ├── ark_tx.go
|   |   ├── bch
|   |   |   └── bchutil
|   |   |   ├── address.go
|   |   |   ├── bitpayaddr.go
|   |   |   ├── bitpayaddr_test.go
|   |   |   ├── cashaddr.go
|   |   |   ├── cashaddr_test.go
|   |   |   ├── protocol.go
|   |   |   ├── seeds.go
|   |   |   ├── sign.go
|   |   |   └── sign_test.go
|   |   ├── bitcoin
|   |   |   └── bech32.go
|   |   ├── eos
|   |   |   ├── buyram.go
|   |   |   ├── bw.go
|   |   |   ├── decoder.go
|   |   |   ├── encoder.go
|   |   |   ├── eos_tx.go
|   |   |   ├── eos_tx_test.go
|   |   |   ├── name.go
|   |   |   ├── newaccount.go
|   |   |   ├── pubkey.go
|   |   |   ├── sellram.go
|   |   |   ├── transfer.go
|   |   |   └── tx_factory.go
|   |   ├── eth_tx.go
|   |   ├── ethsign.go
|   |   ├── icx_tx.go
```

```
|   |   ├── nas
|   |   |   ├── base58.go
|   |   |   ├── block.pb.go
|   |   |   ├── nas_tx.go
|   |   |   └── nas_tx_test.go
|   |   ├── neo
|   |   |   ├── bigint.go
|   |   |   ├── neo_tx.go
|   |   |   ├── opcode.go
|   |   |   └── params_builder.go
|   |   ├── okp_tx.go
|   |   ├── okt
|   |   |   ├── address.go
|   |   |   ├── codec.go
|   |   |   ├── dec_coin.go
|   |   |   ├── decimal.go
|   |   |   ├── int.go
|   |   |   ├── key.go
|   |   |   ├── module.go
|   |   |   ├── msg.go
|   |   |   ├── sign.go
|   |   |   ├── std_tx.go
|   |   |   ├── stdsignmsg.go
|   |   |   ├── tx.go
|   |   |   ├── tx_test.go
|   |   |   ├── types.go
|   |   |   └── utils.go
|   |   ├── ont_tx.go
|   |   ├── token
|   |   |   ├── abi.go
|   |   |   ├── big.go
|   |   |   └── ethtoken.go
|   |   ├── tron
|   |   |   ├── Discover.pb.go
|   |   |   ├── Tron.pb.go
|   |   |   ├── TronInventoryItems.pb.go
|   |   |   ├── account_contract.pb.go
|   |   |   ├── api.pb.go
|   |   |   ├── api_grpc.pb.go
|   |   |   ├── asset_issue_contract.pb.go
|   |   |   ├── balance_contract.pb.go
|   |   |   ├── common.pb.go
|   |   |   ├── exchange_contract.pb.go
```

```
|   |   |   ├── market_contract.pb.go
|   |   |   ├── proposal_contract.pb.go
|   |   |   ├── shield_contract.pb.go
|   |   |   ├── smart_contract.pb.go
|   |   |   ├── storage_contract.pb.go
|   |   |   ├── vote_asset_contract.pb.go
|   |   |   └── witness_contract.pb.go
|   |   ├── utxosign.go
|   |   └── zec
|   |       ├── common.go
|   |       ├── common_test.go
|   |       ├── hash.go
|   |       ├── hashcache.go
|   |       ├── msgtx.go
|   |       └── sign.go
|   ├── tron.go
|   ├── tron_test.go
|   ├── tron_token.go
|   ├── tron_token_test.go
|   ├── usdt.go
|   ├── wallet.go
|   ├── waves.go
|   ├── zcash.go
|   └── zen.go
├── core
|   ├── core.go
|   ├── core_test.go
|   ├── mnemonic.go
|   ├── wallet_manager.go
|   └── wallet_manager_test.go
├── go.mod
├── go.sum
├── main.go
├── storage
|   ├── common.go
|   ├── const.go
|   ├── errors.go
|   ├── tokenabi.go
|   └── tx.go
└── util
    ├── base58.go
    ├── encoder
    |   └── encoder.go
    └── util.go
```

4.4 Chrome

4.4.1 keyrings

```
├── KeyringController.js
├── KeyringController.test.js
├── MultipleHDKeyring.js
├── MultipleHDKeyring.test.js
├── MultipleKeyring.md
├── MultipleLedgerBridgeKeyring.js
├── MultipleLedgerBridgeKeyring.test.js
├── MultipleSimpleKeyring.js
├── MultipleSimpleKeyring.test.js
├── MultipleTrezorKeyring.js
├── MultipleTrezorKeyring.test.js
├── chains
|   ├── ethereum
|   |   ├── HDKeyring.js
|   |   ├── HDKeyring.test.js
|   |   ├── SimpleKeyring.js
|   |   └── SimpleKeyring.test.js
|   └── index.js
├── keyringUtils.js
├── keyringUtils.test.js
└── utils
    ├── index.js
    ├── transfer.js
    └── transfer.test.js
```

4.4.2 js-signlayer

```
packages
├── metax-bitcoin
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── bitcoinjs-lib
|   |   |   ├── address.ts
|   |   |   ├── bip66.ts
|   |   |   ├── bufferutils.ts
|   |   |   ├── crypto.ts
|   |   |   ├── index.ts
|   |   |   ├── networks.ts
|   |   |   ├── ops.ts
|   |   |   ├── payments
|   |   |   |   ├── embed.ts
|   |   |   |   ├── index.ts
|   |   |   |   ├── lazy.ts
|   |   |   |   ├── p2ms.ts
|   |   |   |   ├── p2pk.ts
|   |   |   |   ├── p2pkh.ts
|   |   |   |   ├── p2sh.ts
|   |   |   |   ├── p2wpkh.ts
|   |   |   |   └── p2wsh.ts
|   |   |   ├── push_data.ts
|   |   |   ├── script.ts
|   |   |   ├── script_number.ts
|   |   |   ├── script_signature.ts
|   |   |   ├── transaction.ts
|   |   |   ├── types.ts
|   |   |   ├── varuint.d.ts
|   |   |   └── varuint.js
|   |   ├── index.ts
|   |   ├── txBuild.ts
|   |   ├── type.ts
|   |   └── wif.ts
|   ├── tests
|   |   └── btc.test.ts
|   └── tsconfig.json
```

```
├── metax-cosmos
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── amino
|   |   |   ├── aminoRegistry.ts
|   |   |   ├── aminotypes.ts
|   |   |   ├── coins.ts
|   |   |   ├── encoding.ts
|   |   |   └── pubkeys.ts
|   |   ├── encoding.ts
|   |   ├── index.ts
|   |   ├── osmosis
|   |   |   ├── aminotypes.ts
|   |   |   ├── gamm
|   |   |   |   └── v1beta1
|   |   |   |       └── tx.ts
|   |   |   ├── index.ts
|   |   |   └── registry.ts
|   |   ├── registry.ts
|   |   ├── tx.ts
|   |   ├── types
|   |   |   ├── cosmos
|   |   |   |   ├── bank
|   |   |   |   |   └── v1beta1
|   |   |   |   |       └── tx.ts
|   |   |   |   ├── base
|   |   |   |   |   └── v1beta1
|   |   |   |   |       └── coin.ts
|   |   |   |   ├── crypto
|   |   |   |   |   ├── ed25519
|   |   |   |   |   |   └── keys.ts
|   |   |   |   |   ├── multisig
|   |   |   |   |   |   ├── keys.ts
|   |   |   |   |   |   └── v1beta1
|   |   |   |   |   |   └── multisig.ts
|   |   |   |   |   └── secp256k1
|   |   |   |   |       └── keys.ts
|   |   |   |   ├── staking
|   |   |   |   |   └── v1beta1
|   |   |   |   |       └── tx.ts
|   |   |   |   └── tx
```

```
|   |   |   |   ├── signing
|   |   |   |   |   └── v1beta1
|   |   |   |   |   └── signing.ts
|   |   |   |   └── v1beta1
|   |   |   |   └── tx.ts
|   |   |   ├── gogoproto
|   |   |   |   └── gogo.ts
|   |   |   ├── google
|   |   |   |   ├── api
|   |   |   |   |   ├── annotations.ts
|   |   |   |   |   └── http.ts
|   |   |   |   └── protobuf
|   |   |   |   ├── any.ts
|   |   |   |   ├── descriptor.ts
|   |   |   |   ├── duration.ts
|   |   |   |   └── timestamp.ts
|   |   |   └── ibc
|   |   |   └── applications
|   |   |   └── transfer
|   |   |   ├── v1
|   |   |   |   ├── transfer.ts
|   |   |   |   └── tx.ts
|   |   |   └── v2
|   |   |   └── packet.ts
|   |   └── utils
|   |   └── array.ts
|   ├── tests
|   |   └── luna.test.ts
|   └── tsconfig.json
├── metax-crypto
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── abi
|   |   |   ├── abi.js
|   |   |   ├── index.ts
|   |   |   └── util.ts
|   |   ├── base
|   |   |   ├── ascii.ts
|   |   |   ├── base58.ts
|   |   |   ├── base58Check.ts
|   |   |   ├── base64.ts
|   |   |   ├── bech32.ts
|   |   |   ├── bignumber-plus.ts
```

```
|   |   |   ├── hash.ts
|   |   |   ├── helper.ts
|   |   |   ├── hex.ts
|   |   |   ├── hmac.ts
|   |   |   ├── index.ts
|   |   |   ├── precondtion.ts
|   |   |   ├── rlp.ts
|   |   |   └── utf8.ts
|   |   ├── bip32
|   |   |   ├── api.ts
|   |   |   ├── bip32.ts
|   |   |   └── index.ts
|   |   ├── bip39
|   |   |   ├── _wordlists.ts
|   |   |   ├── index.ts
|   |   |   └── wordlists
|   |   |   ├── chinese_simplified.json
|   |   |   ├── chinese_traditional.json
|   |   |   ├── czech.json
|   |   |   ├── english.json
|   |   |   ├── french.json
|   |   |   ├── italian.json
|   |   |   ├── japanese.json
|   |   |   ├── korean.json
|   |   |   ├── portuguese.json
|   |   |   └── spanish.json
|   |   ├── elliptic
|   |   |   ├── curve
|   |   |   |   ├── base.js
|   |   |   |   ├── edwards.js
|   |   |   |   ├── index.js
|   |   |   |   ├── mont.js
|   |   |   |   └── short.js
|   |   |   ├── curves.js
|   |   |   ├── ec
|   |   |   |   ├── index.js
|   |   |   |   ├── key.js
|   |   |   |   └── signature.js
|   |   |   ├── eddsa
|   |   |   |   ├── index.js
|   |   |   |   ├── key.js
|   |   |   |   └── signature.js
```

```
|   |   |   ├── index.ts
|   |   |   ├── precomputed
|   |   |   |   └── secp256k1.js
|   |   |   └── utils.js
|   |   ├── index.ts
|   |   ├── math
|   |   |   ├── decimal.ts
|   |   |   ├── index.ts
|   |   |   └── integers.ts
|   |   └── signutil
|   |   ├── ed25519.ts
|   |   ├── index.ts
|   |   ├── p256.ts
|   |   └── secp256k1.ts
|   ├── tests
|   |   ├── batch.test.ts
|   |   └── crypto.test.ts
|   └── tsconfig.json
├── metax-eos
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── action.ts
|   |   ├── api.ts
|   |   ├── index.ts
|   |   ├── numeric.ts
|   |   ├── serialize.ts
|   |   ├── txBuilder.ts
|   |   └── types.ts
|   ├── tests
|   |   └── eos.test.ts
|   └── tsconfig.json
├── metax-ethereum
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── api.ts
|   |   ├── index.ts
|   |   ├── message.ts
|   |   └── sdk
|   |   ├── eth-sig-util
|   |   |   ├── index.ts
|   |   |   ├── sign-typed-data.ts
|   |   |   └── utils.ts
```

```
|   |   ├── ethereumjs-tx
|   |   |   ├── baseTransaction.ts
|   |   |   ├── eip1559Transaction.ts
|   |   |   ├── eip2930Transaction.ts
|   |   |   ├── index.ts
|   |   |   ├── legacyTransaction.ts
|   |   |   ├── transactionFactory.ts
|   |   |   ├── types.ts
|   |   |   └── util.ts
|   |   ├── ethereumjs-util
|   |   |   ├── account.ts
|   |   |   ├── address.ts
|   |   |   ├── bytes.ts
|   |   |   ├── constants.ts
|   |   |   ├── externals.d.ts
|   |   |   ├── hash.ts
|   |   |   ├── helpers.ts
|   |   |   ├── index.ts
|   |   |   ├── rlp.ts
|   |   |   ├── signature.ts
|   |   |   ├── types.ts
|   |   |   └── util.ts
|   |   └── index.ts
|   ├── tests
|   |   └── eth.test.ts
|   └── tsconfig.json
├── metax-flow
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── account.ts
|   |   ├── enode.ts
|   |   ├── http.ts
|   |   ├── index.ts
|   |   ├── model.ts
|   |   ├── signature.ts
|   |   └── tx.ts
|   ├── tests
|   |   └── flow.test.ts
|   └── tsconfig.json
├── metax-near
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── enums.ts
```

```
|   |   ├── index.ts
|   |   ├── keypair.ts
|   |   ├── serialize.ts
|   |   └── transaction.ts
|   ├── test
|   |   └── near.test.ts
|   └── tsconfig.json
├── metax-polkadot
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── address.ts
|   |   ├── bn.ts
|   |   ├── const.ts
|   |   ├── hex.ts
|   |   ├── index.ts
|   |   ├── is.ts
|   |   ├── object.ts
|   |   ├── string.ts
|   |   ├── tx.ts
|   |   ├── types.ts
|   |   └── u8a.ts
|   ├── tests
|   |   └── dot.test.ts
|   └── tsconfig.json
├── metax-signlayer
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── api.ts
|   |   ├── basic
|   |   |   ├── ed25519.ts
|   |   |   └── typeUtils.ts
|   |   ├── coins
|   |   |   ├── BtcWallet.ts
|   |   |   ├── EthWallet.ts
|   |   |   ├── SolWallet.ts
|   |   |   ├── TrxWallet.ts
|   |   |   └── index.ts
|   |   ├── common.ts
|   |   ├── currency.ts
|   |   ├── error.ts
|   |   ├── index.ts
|   |   └── wallet.ts
```

```
|   ├── tests
|   |   ├── bch.test.ts
|   |   ├── bsv.test.ts
|   |   ├── btc.test.ts
|   |   ├── eth.test.ts
|   |   ├── ltc.test.ts
|   |   ├── sol.test.ts
|   |   ├── trx.test.ts
|   |   └── usdt.test.ts
|   └── tsconfig.json
├── metax-solana
|   ├── jest.config.js
|   ├── package.json
|   ├── src
|   |   ├── api.ts
|   |   ├── index.ts
|   |   └── sdk
|   |   ├── buffer-layout
|   |   |   ├── index.ts
|   |   |   ├── layout.ts
|   |   |   └── utils
|   |   |   ├── base.ts
|   |   |   ├── bigint.ts
|   |   |   ├── decimal.ts
|   |   |   ├── index.ts
|   |   |   ├── native.ts
|   |   |   └── web3.ts
|   |   ├── index.ts
|   |   ├── spl
|   |   |   ├── constants.ts
|   |   |   ├── errors.ts
|   |   |   ├── index.ts
|   |   |   └── instructions
|   |   |   ├── associatedTokenAccount.ts
|   |   |   ├── index.ts
|   |   |   ├── internal.ts
|   |   |   ├── transfer.ts
|   |   |   ├── transferChecked.ts
|   |   |   └── types.ts
|   |   └── web3
|   |   ├── blockhash.ts
|   |   ├── fee-calculator.ts
|   |   ├── index.ts
```

```
|   |   ├── instruction.ts
|   |   ├── keypair.ts
|   |   ├── layout.ts
|   |   ├── message.ts
|   |   ├── nonce-account.ts
|   |   ├── publickey.ts
|   |   ├── stake-program.ts
|   |   ├── system-program.ts
|   |   ├── sysvar.ts
|   |   ├── transaction-constants.ts
|   |   ├── transaction.ts
|   |   └── util
|   |   ├── assert.ts
|   |   ├── bigint.ts
|   |   ├── borsh-schema.ts
|   |   ├── cluster.ts
|   |   ├── promise-timeout.ts
|   |   ├── shortvec-encoding.ts
|   |   ├── sleep.ts
|   |   ├── to-buffer.ts
|   |   ├── tx-expiry-custom-errors.ts
|   |   └── url.ts
|   ├── tests
|   |   └── sol.test.ts
|   └── tsconfig.json
└── metax-tron
    ├── jest.config.js
    ├── package.json
    ├── src
    |   ├── index.ts
    |   ├── protobuf
    |   |   ├── Contract.proto
    |   |   ├── Discover.proto
    |   |   ├── tron.d.ts
    |   |   ├── tron.js
    |   |   └── tron.proto
    |   └── tronUtils.ts
    ├── tests
    |   └── trx.test.ts
    └── tsconfig.json
```

審計報告匯總

1. 審計方式

通過清晰地理解該項目的設計目的、運行原理和實現管道，稽核團隊對合約程式碼進行了深入的研究和分析。 在理清各個函數的調用關係的基礎上，對錢包可能存在的漏洞進行了定位及分析。 最終產生問題描述和給出相應的修改意見。

審計方法	Static analysis, Manual Review, Fuzzing Test

2. 審計流程

步驟	操作	詳細內容
1	背景研究	閱讀項目介紹、白皮書、合約源碼等項目方團隊提供的相關信息，確保正確理解項目功能
2	自動化檢測	主要用自動化工具掃描源碼，找到常見的潛在漏洞
3	人工審閱	工程師逐行閱讀代碼，找到潛在漏洞
4	邏輯校對	工程師將對代碼的理解和項目方提供的信息比較，檢查代碼實現是否符合項目白皮書信息
5	測試用例檢測	包括測試用例設計，測試範圍分析、符號執行等
6	優化審查	根據應用場景、調用方式及最新的研究成果從可維護性、安全性及可操作性等方面審查項目

3. 風險分級

風險級別	風險描述
致命	存在致命風險及隱患，需要立即解決
高危	存在高危風險及隱患，將引發相同問題，必須解決
中度	存在中度風險及隱患，可能導致潛在風險，最終仍然需要解決
低危	存在低風險及隱患，指各類處理不當或會引發警告信息的細節，這類問題可暫時擱置
建議	存在可優化的部分，這類問題可以擱置，但建議最終解決

4. 審計結果

編號	審計項目	風險級別	狀態
1	私密金鑰洩露	無	
2	助記詞洩露	無	
3	密碼洩露	無	
4	地址派生不安全	無	
5	亂數不安全	中	已告知
6	簽名不當	無	
7	hash算濾使用不當	中	已告知
8	存儲不安全	無	
9	網絡劫持風險	無	
10	跨域風險	無	
11	偽造簽名風險	無	

編號	審計項目	風險級別	狀態
12	數據隱私洩露	無	
13	鑒權不當	無	
14	關鍵字使用不規範	無	
15	條件判斷不規範	無	
16	變數不規範	無	
17	使用不推薦/過期的方法	中	已告知
18	未遵循基本編碼原則	無	
19	WriteFile許可權過高	中	已告知

上述表格中，狀態欄內容若為「已告知」，則表示審計團隊已告知項目方項目存在的漏洞，但項目方未對漏洞進行修改，或未告知審計團隊漏洞的修改進度。若狀態欄中填寫「已修改」則表示項目方已進行對漏洞的修改，並通過審計團隊確認。

5. 風險項與修改方案

以下部分為審計後得知的風險項相關詳細信息，其中內容包括風險類型、風險級別、問題位置、問題描述、修改建議及項目方反饋。

5.1 Wallet-Core

1. 亂數不安全

位置	文件	風險状态	風險級別
Line 106	bip39.go	⚠️已告知	中風險

① 風險描述

在go語言中亂數函數rand（）不被認為具有加密强度。 攻擊者可能預測這些函數生成的亂數達到攻擊目的。 在CVE-2009-3278明確指出Crypto產品使用rand（）庫函數生成恢復金鑰，存在暴力破解可能。

② 修改建議

建議使用强亂數函數

③ 關聯程式碼

```Go
/**
*/
// NewEntropy will create random entropy bytes
// so long as the requested size bitSize is an appropriate size.
//
// bitSize has to be a multiple 32 and be within the inclusive range of {128, 256}
func NewEntropy(bitSize int) ([]byte, error) {
    err := validateEntropyBitSize(bitSize)
    if err != nil {
            return nil, err
    }
    //@OKLink Audit Description: 使用弱亂數函數rand()
    //@OKLink Audit Solution: 使用强亂數函數
    entropy := make([]byte, bitSize/8)
    _, err = rand.Read(entropy)
    return entropy, err
}
```

2. hash算濾使用不當

位置	文件	風險状态	風險級別
Line 1973	opcode.go	⚠️已告知	中風險

① 風險描述

在go庫檔案中表示SHA-1算濾已被破解，不應用於安全應用程序。

② 修改建議

建議使用未破解hash算濾

③ 關聯程式碼

```Go
/**
*/
// opcodeSha1 treats the top item of the data stack as raw bytes and replaces it
// with sha1(data).
//
// Stack transformation: [... x1] -> [... sha1(x1)]
func opcodeSha1(op *parsedOpcode, vm *Engine) error {
    buf, err := vm.dstack.PopByteArray()
    if err != nil {
            return err
    }
---
    //@OKLink Audit Description: 使用已破解hash算灠sha-1
    //@OKLink Audit Solution: 使用未破解hash算灠
---
    hash := sha1.Sum(buf)
    vm.dstack.PushByteArray(hash[:])
    return nil
}
```

3. WriteFile許可權過高

位置	文件	風險状态	風險級別
Line 99	signif.go	⚠️已告知	中風險

① 風險描述

當WriteFile許可權過高，攻擊者可能能够創建或覆蓋用於執行程式碼的關鍵檔案，例如程式、庫或重要數據。 攻擊者也可能讀取意外檔案的內容並暴露敏感數據。 在SignFile函數中WriteFile用做對傳入檔案的簽名輸出，低許可權能保持正常功能運行，高許可權存在風險可能。

② 修改建議

建議WriteFile許可權應小於等於600

③ 關聯程式碼

Go
```
/**
*/
// SignFile creates a signature of the input file.
//
// This accepts base64 keys in the format created by the 'signify' tool.
// The signature is written to the 'output' file.
func SignFile(input string, output string, key string, untrustedComment string,
trustedComment string) error {
    ...

    // Create the main data signature.
    rawSig := ed25519.Sign(skey, filedata)
    var dataSig []byte
    dataSig = append(dataSig, header...)
    dataSig = append(dataSig, keyNum...)
    dataSig = append(dataSig, rawSig...)

    // Create the comment signature.
    var commentSigInput []byte
    commentSigInput = append(commentSigInput, rawSig...)
    commentSigInput = append(commentSigInput, []byte(trustedComment)...)
    commentSig := ed25519.Sign(skey, commentSigInput)
    //@OKLink Audit Description: WriteFile許可權過高
    //@OKLink Audit Solution: WriteFile許可權應小於等於600
    // Create the output file.
    var out = new(bytes.Buffer)
    fmt.Fprintln(out, "untrusted comment:", untrustedComment)
    fmt.Fprintln(out, base64.StdEncoding.EncodeToString(dataSig))
    fmt.Fprintln(out, "trusted comment:", trustedComment)
    fmt.Fprintln(out, base64.StdEncoding.EncodeToString(commentSig))
    return ioutil.WriteFile(output, out.Bytes(), 0644)
}
```

5.2 Chrome

1. 使用不推薦/過期的方法

位置	文件	風險状态	風險級別
Line24, Line1123, Line6187	js-signlayer: packages/metax-crypto/package.json	⚠已告知	中風險

① 風險描述

庫過期問題，加密庫使用的elliptic過期包版本（6.4.14）會引入以下三個漏洞，包含兩個中危一個高危。

中危： https://security.snyk.io/vuln/SNYK-JS-ELLIPTIC-1064899
私密金鑰洩露：通過elliptic/ec/key. js中的secp256k1實現，此套裝軟體的受影響版本容易受到加密問題的攻擊。 沒有檢查以確認傳遞到派生函數中的公開金鑰點實際上存在於secp256k1曲線上。 這導致在執行多個ECDH操作後，可能會顯示此實現中使用的私密金鑰。

中危： https://security.snyk.io/vuln/SNYK-JS-ELLIPTIC-511941
私密金鑰洩露：在某些條件下，可以實際恢復庫生成的長期私密金鑰。 在標量乘法期間，在橢圓曲線上可能出現標量的比特長度洩漏，這可能允許實際恢復長期私密金鑰。

高危： https://security.snyk.io/vuln/SNYK-JS-ELLIPTIC-571484
elliptic允許ECDSA簽名通過編碼變化、前導\0位元組或整數溢出進行延展。 如果應用程序依賴於單個規範簽名，這可能會產生與安全相關的影響。

② 修改建議

建議更改包版本為6.5.4

③　關聯程式碼

```
Json/**
*//
"devDependencies": {
    ...
    "@types/elliptic": "6.4.14",
    ...
  }
  "node_modules/@types/elliptic": {
    "version": "6.4.14",
    "resolved": "https://registry.npmmirror.com/@types/elliptic/-/elliptic-6.4.14.tgz",
    "integrity": "sha512-z4OBcDAU0GVwDTuwJzQCiL6188QvZMkvoERgcVjq0/
mPM8jCfdwZ3x5zQEVoL9WCAru3aG5wl3Z5Ww5wBWn7ZQ==",
    "dev": true,
    "dependencies": {
      "@types/bn.js": "*"
    }
  },
  "@types/elliptic": {
    "version": "6.4.14",
    "resolved": "https://registry.npmmirror.com/@types/elliptic/-/elliptic-6.4.14.tgz",
    "integrity": "sha512-z4OBcDAU0GVwDTuwJzQCiL6188QvZMkvoERgcVjq0/
mPM8jCfdwZ3x5zQEVoL9WCAru3aG5wl3Z5Ww5wBWn7ZQ==",
    "dev": true,
    "requires": {
      "@types/bn.js": "*"
    }
},
```

6. 版本安全優勢

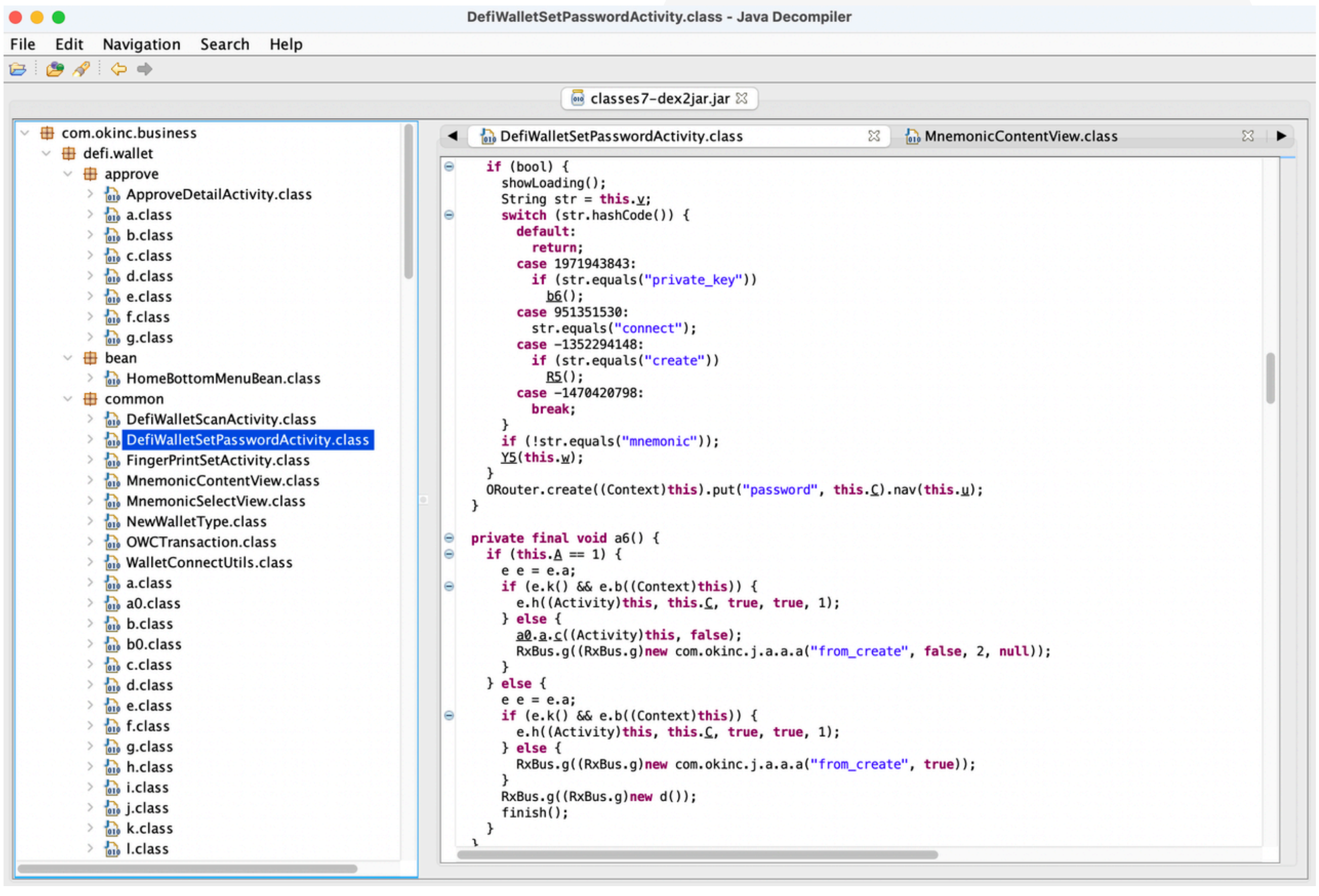
以下部分為審計該版本后得出的採取多維度手段加固達到安全優勢

6.1 Android

稽核未發現明顯漏洞，亂數和網絡請求部分均符合安全要求。 常規安全加固方面符合基本安全要求

6.1.1 程式碼混淆

程式碼已進行混淆，防止反編譯出原始程式碼。



6.1.2 簽名證書

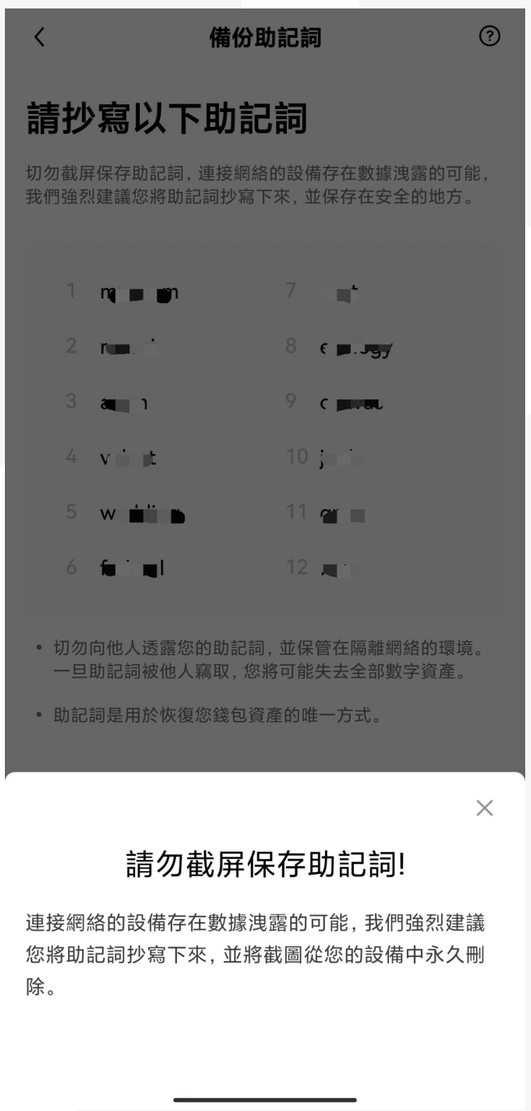
APP使用了正式證書進行簽名，不是使用的debug版本證書。

```
(base) oker@okerdembp-137 okx-android % keytool --printcert --file META-
INF/CERT.RSA
Owner: CN=OK inc., OU=OK inc., O=OK inc., L=Beijing, ST=Beijing, C=CN
Issuer: CN=OK inc., OU=OK inc., O=OK inc., L=Beijing, ST=Beijing, C=CN
Serial number: 3bd2d760
Valid from: Tue Dec 20 15:39:29 CST 2016 until: Thu Nov 26 15:39:29 CST
2116
Certificate fingerprints:
         SHA1: 46:17:0C:99:DC:92:90:BA:D5:F3:CD:F6:C1:30:D8:42:5D:93:6D:77
         SHA256:
77:B9:67:49:D8:F5:A4:F0:79:AB:17:36:18:4A:1B:D2:87:0D:02:CA:14:CD:1C:A9:FF
:BD:A8:1A:CB:65:10:E9
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 47 E8 D6 8A 5C E3 77 F8  1F 28 49 7D C6 BF 9F 36 G...\.w..(I....6
0010: DE 2D 41 1D                                      .-A.
]
]
```

6.1.3 行為分析

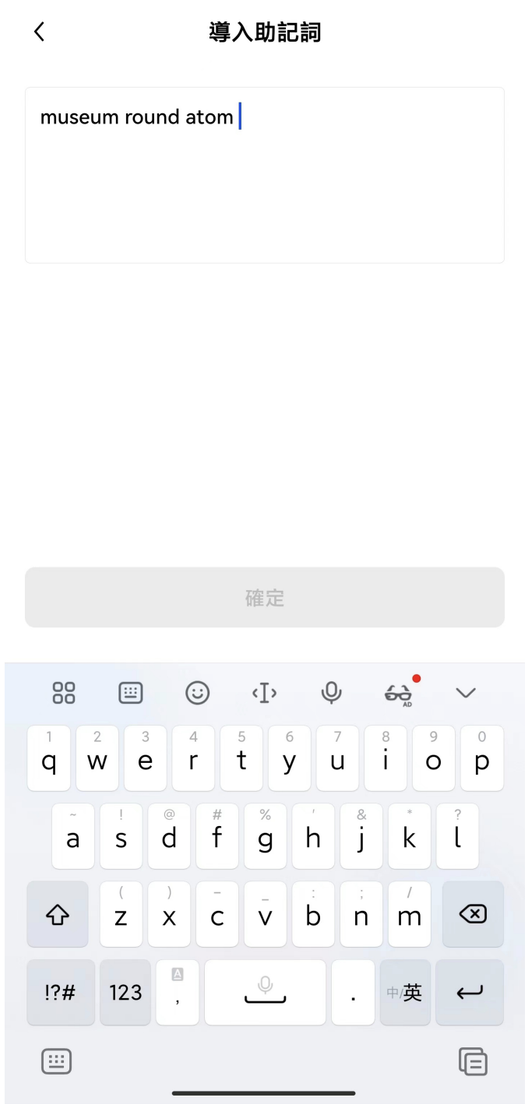
i. 截圖限制

有截圖提醒，但是沒有限制截圖，助記詞有洩漏風險。 建議新增截圖檢測並限制截圖功能。



ii. 安全鍵盤

輸入助記詞未採用安全鍵盤，助記詞有洩露風險。 建議輸入密碼，助記詞等關鍵資訊時，採用安全鍵盤實現，防止關鍵資訊洩漏。



6.2 IOS

稽核未發現明顯漏洞，亂數和網絡請求部分均符合安全要求。

IOS關聯程式碼

Objective-C/**
*//
// OKWMnemonic.m
// OKWalletDeFi
//
// Created by Lydia on 2021/6/21.
//

```
#import "OKWMnemonic.h"
#import "OKWBridge.h"

@implementation OKWQuestion

@end

@implementation OKWMnemonic
+ (NSString*)normalizePhrase:(NSString*)phrase {
    ...
}

+ (OKWMnemonic *)createMnemonic:(NSString *)phrase {
    ...
}
```

//@OKLink Audit Description: 未保存用戶助記詞

```
+ (OKWMnemonic *)createNewMnemonic {
    OKWBridgeResult* result = [OKWBridge randomMnemonic:@"english"];
    return [[OKWMnemonic alloc] initWithPhrase:result.result language:@"english"];
}

+ (NSArray<NSString *> *)getWordList {
    return [OKWBridge getWordList:@"english"].result;
}

- (instancetype)initWithPhrase:(NSString *)phrase language:(NSString *)language {
    ...
}

- (NSArray*)getRandomFrom:(NSArray<NSString*>*)list count:(NSInteger)count excludes:
(NSArray*)excludes {
    NSSet* excludesSet = [NSSet setWithArray:excludes];

    NSMutableArray* result = [NSMutableArray array];
    NSUInteger length = list.count;
    NSMutableDictionary* token = [NSMutableDictionary dictionary];
    while (count > 0) {
```

//@OKLink Audit Description: 使用*arc4random*偽亂數發生器，不暴露*seed*，精度和安全性得到保障

```
        NSInteger x = arc4random() % length;
        NSInteger index = x;
        if (token[@(x)]) {
            index = [token[@(x)] integerValue];
        }
        NSString* str = list[index];
        if (![excludesSet containsObject:str] && ![result containsObject:str]) {
            count--;
            length--;
            [result addObject:str];
            token[@(index)] = token[@(length)] ?: @(length);
        }
    }
    return result;
}

@end
```

6.3 Chrome

6.3.1 行為分析

Chrome挿件共有以下幾種請求：

i. 數據讀取（未發現問題）

- 請求代幣價格數據

	POST /v1/deposit/plugin/market HTTP/1.1
Host	wallet.okex.org
Connection	keep-alive
Content-Length	150
sec-ch-ua	"Chromium":v="104","NotA;Brand":v="99","MicrosoftEdge":v="104"
plugin-version	2.8.0
currency	usd
x-cdn	https://static.coinall.Itd
devid	b021598e-4fc3-497d-bf8b-6c61273fa9c1
locale	zh_CN
User-Agent	Mozilla/5.0(Macintosh;IntelMacOSX10_15_7)AppleWebKit/537.36(KHTML,likeGecko)Chrome/104.0.5112.81Safari/537.36Edge/104.0.1:
Content-Type	application/json;charset=UTF-8
Accept	application/json,text/plain,*/*
sec-ch-ua-mobile	?0
plugin-build-	aed5-08-05-14:02
sec-ch-ua-platform	"macOS"
Origin	chrome-extension://mcohilncbfahbmgdjkbpemcciiolgcge
Sec-Fetch-Site	none
Sec-Fetch-Mode	cors
Sec-Fetch-Dest	empty
Accept-Encoding	gzip,deflate,br
Accept-Language	zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie	locale=zh_CN;aliyungf_tc=a58a3951349e383f285aa82bfc51776e69ce4c4976f2e6dc427a322d91ba4410

請求：https://wallet.okex.org/v1/deposit/plugin/market

返回（見程式碼）：

關聯程式碼

```
Json/**
*//
{
    "code": 0,
    "msg": "",
    "error_code": "0",
    "error_message": "",
    "detailMsg": "",
    "data": [{
            "coinId": 1,
            "currency": "usd",
            "currencyAmount": "24518.5"
    }, {
            "coinId": 822,
            "currency": "usd",
            "currencyAmount": "21.53"
    }, ...]
}
```

- 請求國家資訊

	GET /v3/users/mobile/support/common/check-country-limit?type=2 HTTP/1.1
Host	wallet.okex.org
Connection	keep-alive
sec-ch-ua	"Chromium";V="104", " Not A;Brand";v="99", "Microsoft Edge";V="104"
plugin-version	2.8.0
x-cdn	https://static.okx.com
devid	b021598e-4fc3-497d-bf8b-6c61273fa9c1
locale	zh_CN
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36Edge/104.0.1:
Accept	application/json, text/plain,
sec-ch-ua-mobile	?0
plugin-build-	aed5-08-05-14:02
sec-ch-ua-platform	"macOS"
Sec-Fetch-Site	none
Sec-Fetch-Mode	cors
Sec-Fetch-Dest	empty
Accept-Encoding	gzip, deflate, br
Accept-Language	zh-CN,zh;q=0.9,en;q=0.8,en-GB:q=0.7,en-US;q=0.6
Cookie	locale=zh_CN;aliyungf_tc=a58a3951349e383f285aa82bfc51776e69ce4c4976f2e6dc427a322d91ba4410

請求：https://wallet.okex.org/v3/users/mobile/support/common/check-country-limit?type=2

返回（見程式碼）：

關聯程式碼

```
Json/**
*//
{
    "code": 0,
    "data": {
            "cefi": null,
            "web3": {
                    "country": "CN",
                    "displayCountryName": "中国",
                    "kycLevel": 0,
                    "limit": false,
                    "politStatus": 0,
                    "province": "",
                    "provinceCode": ""
            }
    },
    "detailMsg": "",
    "error_code": "0",
    "error_message": "",
    "msg": ""
}
```

- 請求NFT數據

請求：https://wallet.okex.org/priapi/v1/nft/wallet/plugin/queryCollectedNfts?address=0x115cdafa75447213aa8c03f899ecefa519495f20&project=&chain=&saleStatus=&pageNo=1&pageSize=1000

返回（見程式碼）：

關聯程式碼

Json/**
*//

```
{
    "code": 0,
    "data": {
            "cursor": "",
            "list": [{
                    "bestOffer": null,
                    "certificateFlag": 0,
                    "chain": 137,
                    "chainIcon": "https://static.okx.com/cdn/assets/imgs/223/EA2F7582FE6CA66B.png?x-oss-process=image/format,webp/resize,w_300",
                    "chainName": "Polygon",
                    "collectionName": "east-rfox-collection",
                    "contractAddress": "0x3a2d9ed0bbc72fc480037857a0edfb8bf1b0eca7",
                    "coverUrl": "",
                    "favCount": 0,
                    "id": 5848142524198055,
                    "imxStatus": "",
                    "info": "The RFOX is a metaverse for retail. We combine an immersive retail experience with elements of gaming, social media, and digital events, all built on Virtual Reality and with mobile users in mind. Welcome to the future of connectivity. Visit [our site](https://rfoxnft.site) to invest more",
                    "isFav": false,
                    "lastPrice": null,
                    "name": "RFOX_VALT SHOP PIX_12 #1",
                    "newNft": false,
                    "ownerAddress": "0xc4cb172e4e781a5889b9fa423d78d78920162f6e",
                    "project": 426105,
                    "projectName": "East RFOX Collection",
                    "rankNum": null,
                    "rarity": [],
                    "resourceType": 1,
                    "resourceUrl": "https://static.okx.com/cdn/nft/02f77534-8483-4a2d-a99c-b7d73dea2126.gif?x-oss-process=image/resize,w_300,h_300/format,gif",
                    "sale": null,
                    "status": "",
                    "tack": 0,
                    "tokenId": "1",
                    "tokenStandard": 2,
                    "total": 1,
                    "txns": 0
            },...
    }
}
```

ii. 以轉帳交易為例的交易json發送（未發現數據洩露）

第一次請求（見程式碼）：

第二次請求：發送交易（見程式碼）：

第三次請求：獲取交易狀態（見程式碼）：

第四次請求（見程式碼）：

關聯程式碼

Json/**
*//
第一次請求:


```
{
        "arg": {
                "channel": "wallet-asset"
        },
        "data": {
                "address": "0x115cdafa75447213aa8c03f899ecefa519495f20",
                "baseCoinId": 0,
                "chainId": 1,
                "coinAmount": 645982817148801,
                "coinAmountDec": 0.000645,
                "coinAmountOriginalDec": "0.000645982817148801",
                "coinId": 3,
                "currencyAmount": 1.282062717710711,
                "dailyChange": 0,
                "decimalNum": 18,
                "isCustomToken": false,
                "isNativeToken": true,
                "logo": "https://static.coinall.ltd/cdn/wallet/logo/ETH-20220328.png",
                "name": "Ethereum",
                "symbol": "ETH",
                "tokenAddress": "",
                "type": "",
                "vDecimalNum": 6
        }
}
```

關聯程式碼

```Json
/**
*//
第二次請求:發送交易
{
    "arg": {
        "channel": "wallet-transaction"
    },
    "data": {
        "address": "0x115cdafa75447213aa8c03f899ecefa519495f20",
        "chainDecimalNum": 18,
        "chainSymbol": "ETH",
        "chainVdecimalNum": 6,
        "coinAmount": 0.000100000000000000,
        "coinAmountNum": 100000000000000,
        "coinId": 3,
        "coinSymbol": "ETH",
        "confirmedCount": 0,
        "currencyAmount": 0.105924147956271 27,
        "decimalNum": 18,
        "deleteSwitch": true,
        "direction": 2,
        "from": "0x115cdafa75447213aa8c03f899ecefa519495f20",
        "gasLimit": 21000,
        "gasPrice": 13918000000,
        "isOkexWallet": true,
        "isShowCancel": false,
        "isShowPending": false,
        "isShowSpeedUp": false,
        "isShowSpeedupCancel": false,
        "network": "Ethereum",
        "nonce": 62,
        "priorityFee": 0,
        "repeatTxType": 0,
        "rowId": "1660482550000",
        "serviceCharge": 292278000000000,
        "showCancel": false,
        "showPending": false,
        "showSpeedUp": false,
        "showSpeedupCancel": false,
        "to": "0x8e4cf799b68f01f3a54c7154eeb1d94cc26fbce9",
        "totalConfirm": 12,
        "txId": "4G94nIIBtvh3TkmG-AiD",
        "txSource": 1,
        "txStatus": 2,
        "txTime": 1660482550000,
        "txType": 2,
        "txhash": "0x2223cd17dcd46e679469fb0a8d83723ef5374a2290826512184ba04779b9f765",
        "url": "https://www.oklink.com/eth/tx/
0x2223cd17dcd46e679469fb0a8d83723ef5374a2290826512184ba04779b9f765",
        "vdecimalNum": 6
    }
}
```

關聯程式碼

Json/**
*//
第三次請求：獲取交易狀態


```
{
    "arg": {
            "channel": "wallet-tx-status-toast"
    },
    "data": {
            "address": "0x115cdafa75447213aa8c03f899ecefa519495f20",
            "pushToastCode": 3,
            "pushToastParams": ["0.0001", "ETH"],
            "txHash":
"0x2223cd17dcd46e679469fb0a8d83723ef5374a2290826512184ba04779b9f765",
            "txId": "4G94nIIBtvh3TkmG-AiD",
            "txStatus": 4,
            "url": "https://www.oklink.com/eth/tx/
0x2223cd17dcd46e679469fb0a8d83723ef5374a2290826512184ba04779b9f765"
    }
}
```


第四次請求：


```
{
    "arg": {
            "channel": "wallet-asset"
    },
    "data": {
            "address": "0x115cdafa75447213aa8c03f899ecefa519495f20",
            "baseCoinId": 0,
            "chainId": 1,
            "coinAmount": 645982817148801,
            "coinAmountDec": 0.000645,
            "coinAmountOriginalDec": "0.0006459828171488 01",
            "coinId": 3,
            "currencyAmount": 1.28206271771071088067,
            "dailyChange": 0,
            "decimalNum": 18,
            "isCustomToken": false,
            "isNativeToken": true,
            "logo": "https://static.coinall.ltd/cdn/wallet/logo/ETH-20220328.png",
            "name": "Ethereum",
            "symbol": "ETH",
            "tokenAddress": "",
            "type": "",
            "vDecimalNum": 6
    }
}
```

免責聲明

i. 本審計報告僅針對最終出具報告中載明的審計類型進行審計，其他未知安全漏洞不在本次審計責任範圍之內，我方無需為此承擔責任。

ii. 我方僅應根據審計報告發布之前存在或發生的攻擊或漏洞發布審計報告。對於將來存在或發生的新攻擊或漏洞，我方無法確定對其項目安全狀態的可能影響，對此概不負責。

iii. 我方發布的審計報告中的安全審計分析及其他內容應僅基於項目方在發布審計報告之前向我方提供的文件和材料（包括但不限於合約代碼），並且上述文件和資料不應該存在缺乏信息、被篡改、刪除或隱藏的情況，如果項目方提供的文件和資料存在不真實、不準確、缺乏信息、被篡改、刪除或隱藏的情況，或者對上述文件和資料的改動是在發布審計報告之後作出的，我方不承擔因反映情況與實際情況不一致引起的損失和不利影響 。

iv. 項目方知曉我方出具的審計報告系根據項目方提供的文件和資料、依靠我方現掌握的技術而作出的。但由於任何機構均存在技術的局限性，我方作出的審計報告仍存在無法完整檢測出全部風險的可能性。我方審計團隊鼓勵項目的開發團隊以及任何相關利益方對項目進行後續的測試及審計。

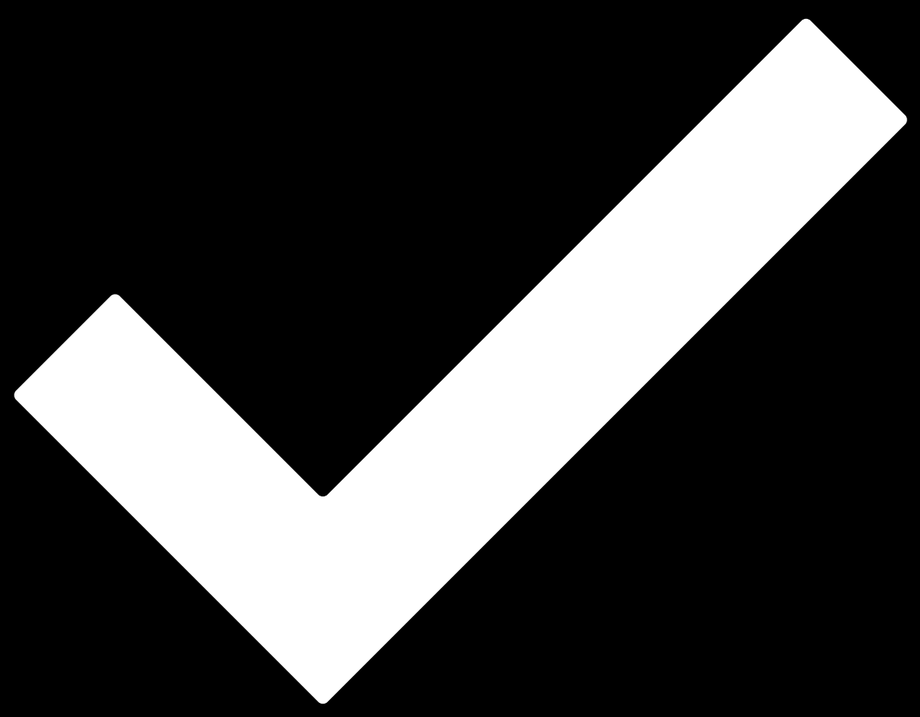
v. 項目方保證其委托我方提供審計或測試服務的項目合法、合規，且不違反適用法律。審計報告僅用於項目方參考，審計報告的內容、獲取方式、使用以及任何其所涉及的服務或資源都不能作為任何形式的投資、稅務、法律、監管及建議等的依據，我方不因此承擔相關責任。在未經我方書面同意之前，項目方不得將審計報告的全部或部分內容以任何形式提及、引用、展示或發送給任何第三方，否則由此產生的任何損失和責任由項目方自行承擔。我方對任何人依賴審計報告或將之用於任何目的概不承擔責任 。

vi. 本審計報告不涉及合約的編譯器及任何超出智能合約編程語言的領域，所審計的智能合約因引用鏈下信息或資源所導致的風險及責任，由項目方自行承擔 。

vii. 不可抗力。不可抗力是指雙方在訂立合同時不能預見、對其發生和後果不能避免且不能克服的事件，包括但不限於戰爭、臺風、水災、火災、地震、潮汐、雷電、天災、罷工、核爆炸、流行病等自然災害和法律、法規和政策變更及政府行為等其它不可預見，對其發生和後果不能防止或避免的事件，且該事件妨礙、影響或延誤任何一方根據合同履行其全部或部分義務。

viii. 如果有一方認為不可抗力發生影響履行本協議義務，應迅速通知另一方，按事件對履約影響的程度，由雙方協商決定是否終止合同或部分免除履約的責任，或者延期履約。

ix. 當不可抗力發生時，任何一方都不能被視作違約或不履行本協議義務。在事件前存在的經濟上的責任，不應受到影響，項目方應對我方已完成工作做出支付。



審計通過.

日期 2022年8月15日

審計 歐科雲鏈

本次稽核主要涵蓋Android、IOS和Chrome流覽器外掛程式端的實現程式碼中用戶助記詞生成、私密金鑰創建、導入、加密存儲和解密私密金鑰進行網絡簽名交易的部分。 稽核的主要目的是通過靜態分析和模糊測試的方法，結合人工稽核，給出Web3錢包的三種用戶端軟體在用戶私密金鑰保護和簽名交易等方面的安全性結論。