

鲲鹏公有链钱包对接指南

鲲鹏公有链(KPG)在比特币代码的技术上融合了以太坊的智能合约功能，其实现方式主要借鉴于量子链。

KPG 拥有和比特币一致的交易结构，支持 P2PK/P2PKH/P2SH等交易类型，支持bech32地址，支持多重签名，支持segwit。

KPG 拥有和比特币基本一致的RPC接口。

KPG 创建交易采用的签名算法和比特币一致。

基本信息

- 官网：<https://kunpeng.network/>
- github：<https://github.com/kunpengproject/kpgchain>
- 浏览器(基于blockbook)：<https://explorer.kunpeng.network/>
- BIP44 Type: 492 <https://github.com/satoshi-labs/slips/blob/master/slip-0044.md>
- 创世块哈希: c895f7e0f717033025778ec38c5d46104e707ec492f4578b786e95d99f30377f
- Base58 PUBKEY_ADDRESS Prefix: 0x2d
- Base58 SCRIPT_ADDRESS Prefix: 0x38
- Base58 SECRET_KEY Prefix: 0x80
- base58Prefixes[EXT_PUBLIC_KEY] = {0x04, 0x88, 0xB2, 0x1E}
- base58Prefixes[EXT_SECRET_KEY] = {0x04, 0x88, 0xAD, 0xE4}
- bech32_hrp = kp

KPG在数据结构方面和比特币的主要区别

1. 区块头，新增了 hashStateRoot[32] hashUTXORoot[32] prevoutStake[4] vchBlockSig[不定长 array], <https://github.com/kunpengproject/kpgchain/blob/master/src/primitives/block.h>
2. ScriptPubKey中新增了 OP_CALL / OP_CREATE / OP_SENDER / OP_SPEND 四个操作码用于支持智能合约。<https://github.com/kunpengproject/kpgchain/blob/master/src/script/script.h>