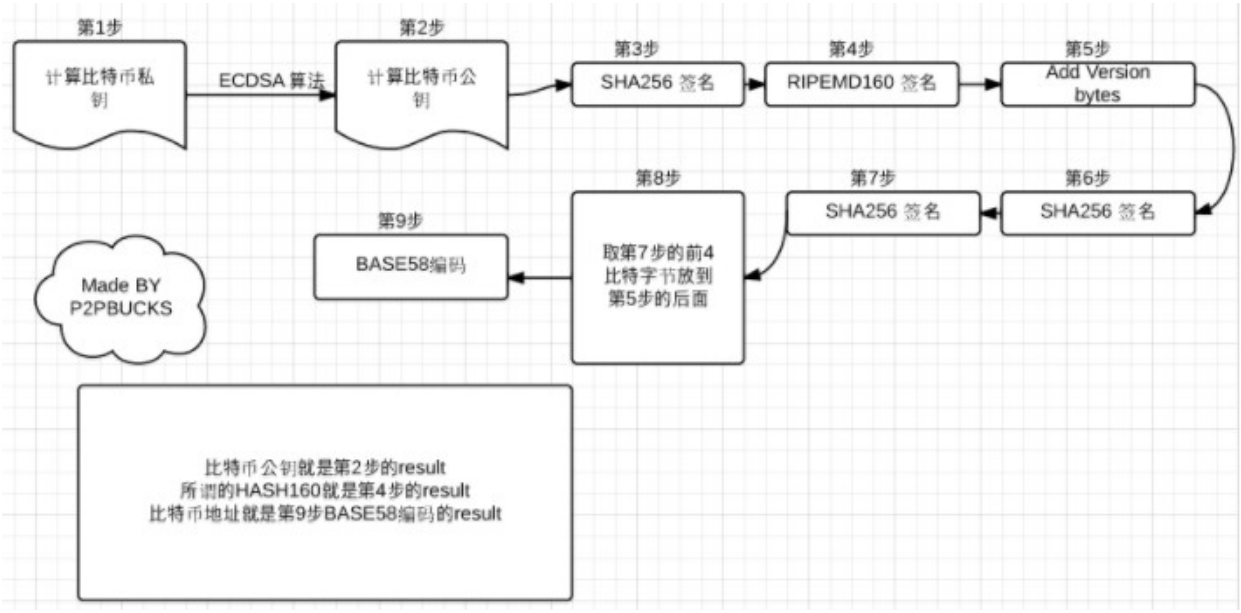

第一步，随机选取一个 32 字节的数，大小介于 1~0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4141 之间，作为私钥
18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725

第二步，使用椭圆曲线加密算法（ECDSA-SECP256k1）计算私钥所对应的非压缩公钥（共 65 字节，1 字节 0x04，32 字节为 x 坐标，32 字节为 y 坐标）。
0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6

第三步，计算公钥的 SHA-256 哈希值
600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B408

第四步，计算上一步哈希值的 RIPEMD-160 哈希值 010966776006953D5567439E5E39F86A0D273BEE

第五步，在上一步结果之间加入地址版本号（如比特币主网版本号"0x00"）
00010966776006953D5567439E5E39F86A0D273BEE

第六步，计算上一步结果的 SHA-256 哈希值
445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094

第七步，再次计算上一步结果的 SHA-256 哈希值
D61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30

第八步，取上一步结果的前 4 个字节（8 位十六进制数）D61967F6，把这 4 个字节加在第五步结果的后面，作为校验（这就是比特币地址的 16 进制形态）
00010966776006953D5567439E5E39F86A0D273BEED61967F6

第九步，用 base58 表示法变换一下地址（这就是最常见的比特币地址形态）
16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

 # 非压缩公钥:
private_key: 18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725 64
public_key:
0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6 130
pub to sha256: 600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B40864
to ripemd160: 010966776006953D5567439E5E39F86A0D273BEE 40
add '0x00': 00010966776006953D5567439E5E39F86A0D273BEE 42
to sha256: 445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094 64
sha256_sha256:
D61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30 64
address_hex: 00010966776006953D5567439E5E39F86A0D273BEED61967F6 50
address: 16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM 33

 # 压缩公钥:
private_key: 18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725 64
public_key: 0250863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B235266
pub to sha256: 0B7C28C9B7290C98D7438E70B3D3F7C848FBD7D1DC194FF83F4F7CC9B1378E9864
to ripemd160: F54A5851E9372B87810A8E60CDD2E7CFD80B6E31 40
add '0x00': 00F54A5851E9372B87810A8E60CDD2E7CFD80B6E31 42
to sha256: AD3C854DA227C7E99C4ABFAD4EA41D71311160DF2E415E713318C70D67C6B41C 64
sha256_sha256: C7F18FE8FCBED6396741E58AD259B5CB16B7FD7F041904147BA1DCFFABF747FD64
address_hex: 00F54A5851E9372B87810A8E60CDD2E7CFD80B6E31C7F18FE8 50
address: 1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs 34