پیوست الف

عملگرها، ثابت‌ها و نمادهای زبان «اسکریپت»

جدول‌های این پیوست از https://en.bitcoin.it/wiki/Script اخذ شده‌اند.

جدول الف-۱ عملگرهای فرستادن مقدار به پشته در زبان «اسکریپت» را نشان می‌دهد.

جدول الف-۱ فرستادن مقدار به داخل پشته

نماد	مقدار (hex)	توضیح
OP_0 یا OP_FALSE	0x00	یک آرایه‌ی خالی به داخل پشته فرستاده می‌شود.
۱ تا ۷۵	0x01–0x4b	N بایت بعدی (N از ۱ تا ۷۵ بایت) را به داخل پشته می‌فرستد.
OP_PUSHDATA1	0x4c	بایت بعدی اسکریپت شامل مقدار N است؛ N بایت بعد از آن را به داخل پشته می‌فرستد.
OP_PUSHDATA2	0x4d	دو بایت بعدی اسکریپت شامل مقدار N هستند؛ N بایت بعد از آنها را به داخل پشته می‌فرستد.
OP_PUSHDATA4	0x4e	چهار بایت بعدی اسکریپت شامل مقدار N هستند؛ N بایت بعد از آنها را به داخل پشته می‌فرستد.
OP_1NEGATE	0x4f	مقدار «۱-» را به داخل پشته می‌فرستد.
OP_RESERVED	0x50	توقف؛ به جز در یک عبارت OP_IF اجرانشده، باعث نامعتبر شدن تراکنش می‌شود.
OP_1 یا OP_TRUE	0x51	مقدار «۱» را به داخل پشته می‌فرستد.
OP_2 تا OP_16	0x52 تا 0x60	در دستوری مانند OP_N (N از ۲ تا ۱۶) مقدار «N» را به داخل پشته می‌فرستد.

جدول الف-۲ عملگرهای شرطی (کنترل جریان اسکریپت) را نشان می‌دهد.

جدول الف-۲ عملگرهای کنترل جریان شرطی

نماد	مقدار (hex)	توضیح
OP_NOP	0x61	هیچ کاری نکن.
OP_VER	0x62	توقف؛ به جز در یک عبارت OP_IF اجرانشده، باعث نامعتبر شدن تراکنش می‌شود.
OP_IF	0x63	اگر مقدار بالای پشته صفر (FALSE) نباشد، دستورات بخش IF را اجرا می‌کند.
OP_NOTIF	0x64	اگر مقدار بالای پشته صفر (FALSE) باشد، دستورات بخش IF را اجرا می‌کند.
OP_VERIF	0x65	توقف؛ باعث نامعتبر شدن تراکنش می‌شود.
OP_VERNOTIF	0x66	توقف؛ باعث نامعتبر شدن تراکنش می‌شود.
OP_ELSE	0x67	اگر دستورات قبلی اجرا نشده باشند، دستورات این بخش را اجرا می‌کند.
OP_ENDIF	0x68	پایان بلوک OP_IF، OP_NOTIF و OP_ELSE.
OP_VERIFY	0x69	مقدار بالای پشته را می‌خواند: اگر TRUE (غیرصفر) نباشد، متوقف شده و تراکنش را نامعتبر می‌کند.
OP_RETURN	0x6a	توقف؛ باعث نامعتبر شدن تراکنش می‌شود.

جدول الف-۳ عملگرهای مورد استفاده در قفل‌های زمانی را نشان می‌دهد.

جدول الف-۳ عملگرهای قفل زمانی

نماد	مقدار (hex)	توضیح
OP_CHECKLOCKTIMEVERIFY (قبلاً OP_NOP2)	0xb1	اگر مقدار بالای پشته بزرگتر از فیلد nLockTime تراکنش باشد، تراکنش را نامعتبر می‌کند؛ در غیر این صورت، اسکریپت با اجرای یک OP_NOP ادامه می‌یابد. همچنین، اگر الف) پشته خالی باشد، ب) مقدار بالای منفی پشته باشد، پ) مقدار بالای پشته بزرگتر یا مساوی 500000000 بوده، در حالی که فیلد nLockTime تراکنش کوچکتر از 500000000 باشد (یا بر عکس)، یا ت) فیلد nSequence ورودی برابر با 0xffffffff باشد، تراکنش نامعتبر می‌شود. کارکرد دقیق این عملگر در BIP-65 توصیف شده است.
OP_CHECKSEQUENCEVERIFY (قبلاً OP_NOP3)	0xb2	اگر قفل زمانی نسبی ورودی (که با فیلد nSequence تعریف می‌شود؛ BIP-68 را ببینید) مساوی یا بزرگتر از مقدار بالای پشته نباشد، تراکنش را نامعتبر می‌کند. کارکرد دقیق این عملگر در BIP-112 توصیف شده است.

جدول الف-۴ عملگرهای مدیریت پشته را نشان می‌دهد.

جدول الف-۴ عملگرهای مدیریت پشته

نماد	مقدار (hex)	توضیح
OP_TOALTSTACK	0x6b	بیرون کشیدن یک درایه از پشته‌ی اصلی و فرستادن آن به پشته‌ی جایگزین.
OP_FORMALTSTACK	0x6c	بیرون کشیدن یک درایه از پشته‌ی جایگزین و فرستادن آن به پشته‌ی اصلی.
OP_2DROP	0x6d	بیرون کشیدن دو درایه از پشته.
OP_2DUP	0x6e	تکرار دو درایه‌ی بالای پشته‌ی.
OP_3DUP	0x6f	تکرار سه درایه‌ی بالای پشته‌ی.
OP_2OVER	0x70	کپی کردن درایه‌های سوم و چهارم پشته در بالای آن.
OP_2ROT	0x71	انتقال درایه‌های پنجم و ششم پشته به بالای آن.
OP_2SWAP	0x72	جابجا کردن دو درایه‌ی بالای پشته با یکدیگر.
OP_IFDUP	0x73	کپی کردن درایه‌ی بالای پشته در صورتی که مقدار آن صفر نباشد.
OP_DEPTH	0x74	شمارش تعداد درایه‌های پشته و فرستادن عدد حاصل به داخل پشته.
OP_DROP	0x75	بیرون کشیدن مقدار بالای پشته.
OP_DUP	0x76	تکرار درایه‌ی بالای پشته‌ی.
OP_NIP	0x77	بیرون کشیدن درایه‌ی دوم از بالای پشته.
OP_OVER	0x78	کپی کردن درایه‌ی دوم پشته و فرستادن آن به بالای پشته.
OP_PICK	0x79	بیرون کشیدن N درایه از بالای پشته، و سپس کپی کردن درایه‌ی N ام در بالای پشته.
OP_ROLL	0x7a	بیرون کشیدن N درایه از بالای پشته، و سپس انتقال درایه‌ی N ام به بالای پشته.
OP_ROT	0x7b	چرخاندن سه درایه‌ی بالای پشته.
OP_SWAP	0x7c	جابجا کردن سه درایه‌ی بالای پشته با یکدیگر.
OP_TUCK	0x7d	کپی کردن درایه‌ی بالای پشته و قرار دادن آن بین درایه‌های اول و دوم پشته.

جدول الف-۵ عملگرهای رشته را نشان می‌دهد.

جدول الف-۵ عملگرهای رشته

نماد	مقدار (hex)	توضیح
OP_CAT	0x7e	غیرفعال (دو درایه‌ی بالای پشته را به هم می‌چسباند).
OP_SUBSTR	0x7f	غیرفعال (یک زیررشته برمی‌گرداند).
OP_LEFT	0x80	غیرفعال (زیررشته‌ی چپ را برمی‌گرداند).
OP_RIGHT	0x81	غیرفعال (زیررشته‌ی راست را برمی‌گرداند).
OP_SIZE	0x82	طول درایه‌ی بالای پشته را محاسبه کرده و عدد حاصل را به داخل پشته می‌فرستد.

جدول الف-۶ عملگرهای حساب باینری و منطق بولی را نشان می‌دهد.

جدول الف-۶ عملگرهای حساب باینری و شرطی

نماد	مقدار (hex)	توضیح
OP_INVERT	0x83	غیرفعال (بیت‌های درایه‌ی بالای پشته را معکوس می‌کند).
OP_AND	0x84	غیرفعال (دو درایه‌ی بالای پشته را AND منطقی می‌کند).
OP_OR	0x85	غیرفعال (دو درایه‌ی بالای پشته را OR منطقی می‌کند).
OP_XOR	0x86	غیرفعال (دو درایه‌ی بالای پشته را XOR منطقی می‌کند).
OP_EQUAL	0x87	اگر دو درایه‌ی بالای پشته دقیقاً برابر باشند، مقدار TRUE (۱)، و در غیر این صورت FALSE (صفر)، به بالای پشته می‌فرستد.
OP_EQUALVERIFY	0x88	مانند OP_EQUAL، با این تفاوت که عملگر OP_VERIFY را نیز اجرا کرده و در صورت TRUE نبودن مقدار بالای پشته، متوقف می‌شود.
OP_RESERVED1	0x89	توقف؛ به جز در یک عبارت OP_IF اجرانشده، باعث نامعتبر شدن تراکنش می‌شود.
OP_RESERVED2	0x8a	توقف؛ به جز در یک عبارت OP_IF اجرانشده، باعث نامعتبر شدن تراکنش می‌شود.

جدول الف-۷ عملگرهای عددی (محاسباتی) را نشان می‌دهد.

جدول الف-۷ عملگرهای عددی

نماد	مقدار (hex)	توضیح
OP_1ADD	0x8b	۱ واحد به درایه‌ی بالای پشته اضافه می‌کند.
OP_1SUB	0x8c	۱ واحد از درایه‌ی بالای پشته کم می‌کند.
OP_2MUL	0x8d	غیرفعال (درایه‌ی بالای پشته را در ۲ ضرب می‌کند).
OP_2DIV	0x8e	غیرفعال (درایه‌ی بالای پشته را بر ۲ تقسیم می‌کند).
OP_NEGATE	0x8f	علامت درایه‌ی بالای پشته را معکوس می‌کند.
OP_ABS	0x90	علامت درایه‌ی بالای پشته را مثبت می‌کند.
OP_NOT	0x91	اگر درایه‌ی بالای پشته 0 یا 1 باشد، آن را معکوس منطقی می‌کند؛ و گرنه، 0 برمی‌گرداند.
OP_0NOTEQUAL	0x92	اگر درایه‌ی بالای پشته 0 باشد، 0، و در غیر این صورت، 1 برمی‌گرداند.
OP_ADD	0x93	دو درایه‌ی بالای پشته را بیرون می‌کشد، و حاصل جمع آنها را به پشته برمی‌گرداند.
OP_SUB	0x94	دو درایه‌ی بالای پشته را بیرون می‌کشد، و حاصل تفریق آنها را به پشته برمی‌گرداند.
OP_MUL	0x95	غیرفعال (دو درایه‌ی بالای پشته را در یکدیگر ضرب می‌کند).
OP_DIV	0x96	غیرفعال (درایه‌ی دوم از بالای پشته را بر درایه‌ی اول تقسیم می‌کند).
OP_MOD	0x97	غیرفعال (باقیمانده‌ی تقسیم درایه‌ی دوم از بالای پشته بر درایه‌ی اول را برمی‌گرداند).
OP_LSHIFT	0x98	غیرفعال (بیت‌های درایه‌ی دوم بالای پشته را به دفعات درایه‌ی اول به چپ انتقال می‌دهد).
OP_RSHIFT	0x99	غیرفعال (بیت‌های درایه‌ی دوم بالای پشته را به دفعات درایه‌ی اول به راست انتقال می‌دهد).

OP_BOOLAND	0x9a	AND منطقی دو درایه‌ی بالای پشته.
OP_BOOLOR	0x9b	OR منطقی دو درایه‌ی بالای پشته.
OP_NUMEQUAL	0x9c	اگر دو درایه‌ی بالای پشته مساوی باشند، TRUE برمی‌گرداند.
OP_NUMEQUALVERIFY	0x9d	مانند OP_NUMEQUAL: سپس OP_VERIFY اجرا شده؛ توقف در صورت TRUE نبودن.
OP_NUMNOTEQUAL	0x9e	اگر دو درایه‌ی بالای پشته مساوی نباشند، TRUE برمی‌گرداند.
OP_LESSTHAN	0x9f	اگر درایه‌ی دوم از بالای پشته کوچکتر از درایه‌ی اول باشد، TRUE برمی‌گرداند.
OP_GREATERTHAN	0xa0	اگر درایه‌ی دوم از بالای پشته بزرگتر از درایه‌ی اول باشد، TRUE برمی‌گرداند.
OP_LESSTHANOREQUAL	0xa1	اگر درایه‌ی دوم از بالای پشته کوچکتر یا مساوی درایه‌ی اول باشد، TRUE برمی‌گرداند.
OP_GREATERTHANOREQUAL	0xa2	اگر درایه‌ی دوم از بالای پشته بزرگتر یا مساوی درایه‌ی اول باشد، TRUE برمی‌گرداند.
OP_MIN	0xa3	از بین دو درایه‌ی بالای پشته، مقدار کوچکتر را برمی‌گرداند.
OP_MAX	0xa4	از بین دو درایه‌ی بالای پشته، مقدار بزرگتر را برمی‌گرداند.
OP_WITHIN	0xa5	اگر درایه‌ی سوم از بالای پشته مابین (یا مساوی) درایه‌های اول و دوم باشد، TRUE برمی‌گرداند.

جدول الف-۸ عملگرهای رمزنگاری را نشان می‌دهد.

جدول الف-۸ عملگرهای رمزنگاری

نماد	مقدار (hex)	توضیح
OP_RIPEMD160	0xa6	دَرهم RIPEMD160 درایه‌ی بالای پشته را برمی‌گرداند.
OP_SHA1	0xa7	دَرهم SHA1 درایه‌ی بالای پشته را برمی‌گرداند.
OP_SHA256	0xa8	دَرهم SHA256 درایه‌ی بالای پشته را برمی‌گرداند.
OP_HASH160	0xa9	دَرهم RIPEMD160(SHA256(x)) درایه‌ی بالای پشته را برمی‌گرداند.
OP_HASH256	0xaa	دَرهم SHA256(SHA256(x)) درایه‌ی بالای پشته را برمی‌گرداند.
OP_CODESEPARATOR	0xab	ابتدای داده‌ی امضادار را مشخص می‌کند.
OP_CHECKSIG	0xac	یک کلید عمومی و امضا از بالای پشته را بیرون می‌کشد، این امضا را برای دَرهم تراکُنش اعتبارسنجی می‌کند؛ اگر منطبق باشد، TRUE برمی‌گرداند.
OP_CHECKSIGVERIFY	0xad	مانند OP_CHECKSIG: سپس OP_VERIFY اجرا شده؛ توقف در صورت TRUE نبودن.
OP_CHECKMULTISIG	0xae	عملگر CHECKSIG را روی تمامی زوج کلید عمومی-امضای داده‌شده اجرا می‌کند؛ همگی باید منطبق باشند. باگ در پیاده‌سازی این عملگر باعث شده تا یک مقدار اضافی از پشته بیرون بکشد، که برای حل آن باید یک OP_NOP به ابتدای اسکریپت اضافه شود.
OP_CHECKMULTISIGVERIFY	0xaf	مانند OP_CHECKMULTISIG: سپس OP_VERIFY: توقف در صورت TRUE نبودن.

جدول الف-۹ عملگرهای غیراجرایی را نشان می‌دهد.

جدول الف-۹ عملگرهای غیراجرایی

نماد	مقدار (hex)	توضیح
OP_NOP1 تا OP_NOP10	0xb0 تا 0xb9	هیچ کاری نمی‌کند؛ نادیده گرفته می‌شود.

جدول الف- ۱۰ عملگرهای رزرو شده برای عملیات تجزیه‌ی اسکریپت (در داخل موتور اسکریپت) را نشان می‌دهد.

جدول الف- ۱۰ عملگرهای رزرو شده برای عملیات تجزیه‌ی اسکریپت (در داخل موتور اسکریپت)

نماد	مقدار (hex)	توضیح
OP_SMALLDATA	0xf9	فیلد داده‌ی کوچک.
OP_SMALLINTEGER	0xfa	فیلد داده‌ی عدد صحیح کوچک.
OP_PUBKEYS	0xfb	چند فیلد کلید عمومی.
OP_PUBKEYHASH	0xfd	یک فیلد دَرهم کلید عمومی.
OP_PUBKEY	0xfe	یک فیلد کلید عمومی.
OP_INVALIDOPCODE	0xff	کُدهای اجرایی که در حال حاضر تعریف نشده‌اند.