Chapter 7 Advanced Transactions and Scripting

P2PKH(pay to pub key hash)

Locking script

OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7
OP_EQUALVERIFY OP_CHECKSIG

Unlock script

<Sig> <Public Key>

Multi signature

Locking Script

M <PubKey 1> <PubKey2> ... <PubKey N> N CHECKMULTISIG

※M是花費輸出所需的簽名的數量

※N是列出的公開金鑰的總數

Unlocking Script

0 <Signature B> <Signature C>

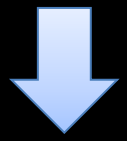
Multi signature

- 比特幣錢包軟體不一定支援
- 額外的腳本長度將造成手續費負擔
- 一個長的交易腳本將一直記錄在所有節點的隨機記憶體的UTXO集中，直到該筆資金被使用

P2SH(Pay-to-Script-Hash)

- 旨在使複雜字串的運用能與直接向比特幣地址支付一樣簡單
- P2SH的含義：向與目標雜湊匹配的腳本支付，當輸出被支付時，該腳本將在後續呈現。

204C16B8698A9ABF84250A7C3EA7EEDEF9897D1C8C6ADF47F06CF73370D74DCCA01CDCA79D
CC5C395D7EEC6984D83F1F50C900A24DD47F569FD4193AF5DE762C58704A2192968D8655D6A
935BEAF2CA23E3FB87A3495E7AF308EDF08DAC3C1FCBFC2C75B4B0F4D0B1B70CD2423657738
C0C2B1D5CE65C97D78D0E34224858008E8B49047E63248B75DB7379BE9CDA8CE5751D16485F
431E46117B9D0C1837C9D5737812F393DA7D4420D7E1A9162F0279CFC10F1E8E8F3020DECDB
C3C0DD389D997796504 21D65CBD7149B255382ED7F78E946580657EE6FDA162A187543A9D85
BAAA93A4AB3A8F044DADA618D087227440645ABE8A35DA8C5B73997AD343BE5C2AFD94A504
3752580AFA1ECED3C68D446BCAB69AC0BA7DF50D56231BE0AABF1FDEEC78A6A45E394BA29A
1EDF518C022DD618DA774D207D137AAB59E0B000EB7ED238F4D800
5 CHECKMULTISIG



HASH160(SHA256+ RIPEMD160)

HASH160 54c557e07dde5bb6cb791c7a540e0a4796f5e97e EQUAL

1. 不含P2SH的複雜字串

Locking Script	2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 5 CHECKMULTISIG
Unlocking Script	0 Sig1 Sig2

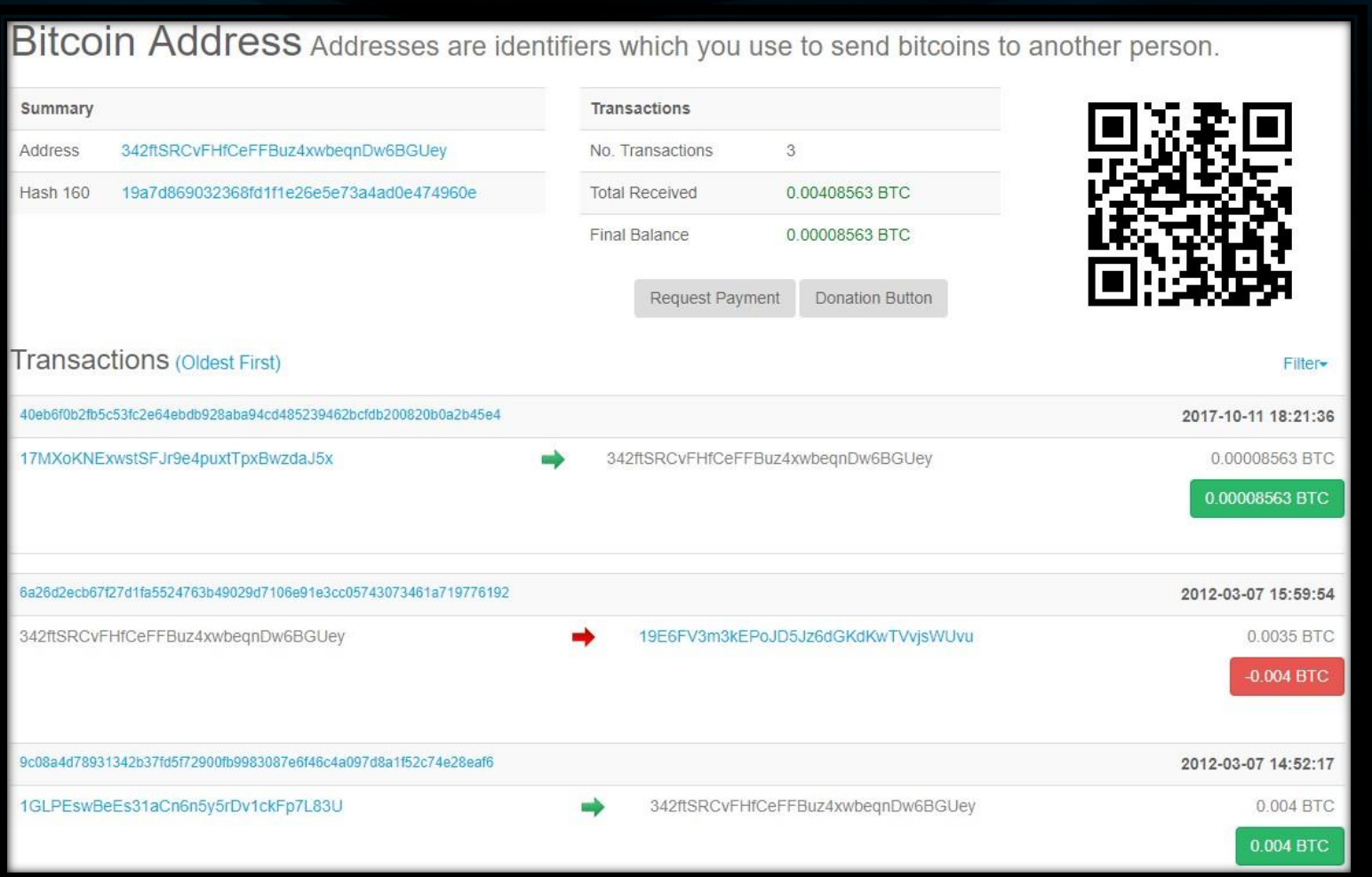
2. P2SH複雜字串

Redeem Script	2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 5 CHECKMULTISIG
Locking Script	HASH160 <20-byte hash of redeem script> EQUAL
Unlocking Script	0 Sig1 Sig2 <2 PK1 PK2 PK3 PK4 PK5 5 CHECKMULTISIG>

- 這使得給礦工的交易費用從發送方轉移到收款方
- 複雜的計算工作也從發送方轉移到收款方

P2SH地址

- P2SH的另一重要特徵是它能將腳本雜湊編譯為一個位址
- P2SH位址19a7d869032368fd1f1e26e5e73a4ad0e474960e
- 經base58編碼342ftSRCvFHfCeFFBuz4xwbeqnDw6BGUey



Address2hash160：https://bitcoinvalued.com/tools.php

P2SH的優點

- 在交易輸出中，複雜字集由簡短電子指紋取代，使得交易代碼變短。
- 腳本能被編譯為位址，支付指令的發出者和支付者的比特幣錢包不需要複雜工序就可以執行P2SH。
- P2SH將構建腳本的重擔轉移至接收方，而非發送方。
- P2SH將長腳本資料存儲的負擔從輸出方（存儲於UTXO集，影響記憶體）轉移至輸入方（存儲在區塊鏈裡面）。
- P2SH將長腳本資料存儲的重擔從當前（支付時）轉移至未來（花費時）。
- P2SH將長腳本的交易費成本從發送方轉移至接收方，接收方在使用該筆資金時必須含有贖回腳本。

資料記錄輸出（RETURN）

- 為檔記錄電子指紋，則任何人都可以通過該機制在特定的日期建立關於文檔存在性的證明。
- 此類交易僅將比特幣位址當作自由組合的20個位元組而使用，進而會產生不能用於交易的UTXO。因為比特幣位址只是被當作資料使用，並不與私密金鑰相匹配

- 在0.9版的比特幣核心用戶端上，通過採用Return操作符最終實現了妥協。
- Return創造了一種明確的可複查的非交易型輸出，此類資料無需存儲於UTXO集
- Return輸出被記錄在區塊鏈上，它們會消耗磁碟空間，也會導致區塊鏈規模的增加，但它們不存儲在UTXO集中，因此也不會使得UTXO記憶體膨脹，更不會以消耗代價高昂的記憶體為代價使全節點都不堪重負。
- RETURN 腳本的樣式：
- RETURN <data>
- “data”部分被限制為80位元組，且多以雜湊方式呈現

- $> bitcoind getrawtransaction 8bae12b5f4c088d940733dcd1455efc6a3a69cf9340e17a981286d3778615684 1


```
{
"hex" : "0100000001c85…ac00000000",
"txid" : "8bae12b5f4c088d940733dcd1455efc6a3a69cf9340e17a981286d3778615684", "version" : 1,
"locktime" : 0,
"vin" : [
        { "txid" : "8e40bb…5fba58c8",
        "vout" : 1,
        "scriptSig" : {
                "asm" : "3045022…",
                "hex" : "4830450…"
                },
                "sequence" : 4294967295
        }
 ],
"vout" : [
        {
                "value" : 0.00000000,
                "n" : 0,
                "scriptPubKey" : {
                        "asm" : "OP_RETURN 636861726c6579206c6f766573206865696469",
                        "hex" : "6a13636861726c6579206c6f766573206865696469",
                        "type" : "nulldata"
                }
        },
],
"blockhash" : "000000000000000004c31376d7619bf0f0d65af6fb028d3b4a410ea39d22554c",
"confirmations" : 2655,
"time" : 1404107109,
"blocktime" : 1404107109
```


636861726c6579206c6f766573206865696469

Hex2bin

http://www.spajz.com/php-functions/hex2bin

charley loves heidi

時間鎖（Timelocks）

- 時間鎖是只允許在一段時間後才允許支出的交易。

	Absolute Timelock	Relative Timelock
Lock Transaction	nTimeLock	nSequence
Lock Output	OP_CHECKLOCKTIMEVERIFY	OP_CHECKSEQUENCEVERIFY

交易鎖定時間（nLocktime）

- $\begin{cases} \text{不鎖定}, & nLocktime = 0 \\ \text{區塊高度}, & \text{nLocktime} < 500{,}000{,}000 \\ \text{Unix紀元時間戳記}, & \text{nLocktime} \geq 500{,}000{,}000 \end{cases}$
- 並且只有在有效後才被發送到比特幣網路。如果交易在指定的nLocktime之前傳輸到網路，那麼第一個節點就會拒絕該交易

nLocktime = 500,000,000　　GMT: 1985年11月5日Tuesday 00:53:20
nLocktime = 1,251,763,200　GMT: 2009年9月1日Tuesday 00:00:00
nLocktime = 1,534,931,644　GMT: 2018年8月22日Wednesday 09:54:04

交易鎖定時間限制

- Alice簽署了一筆交易，支付給Bob的位址，並將交易nLocktime設定為3個月。Alice把這筆交易發送給Bob。有了這個交易，Alice和Bob知道：在3個月過去之前，Bob不能完成交易進行變現。Bob可以在3個月後接受交易。

- 然而：Alice可以創建另一個交易，雙重花費相同的輸入，而不需要鎖定時間。 因此，Alice可以在3個月過去之前花費相同的UTXO。Bob不能保證Alice不會這樣做。

檢查鎖定時間驗證Check Lock Time Verify (CLTV)

- <now + 3 months> CHECKLOCKTIMEVERIFY DROP DUP HASH160 <Bob's Public Key Hash> EQUALVERIFY CHECKSIG
- <now +3個月>是從交易開始被挖礦時間起計3個月的塊高度或時間值
  ：當前塊高度+12,960（塊）或當前Unix紀元時間+7,760,000（秒）
- 通過將nLocktime與CLTV結合使用，交易鎖定時間限制中描述的情況發生變化。因為Alice鎖定了UTXO本身，所以現在Bob或Alice在3個月的鎖定時間到期之前不可能花費它。

相對時間鎖

<+6Months> CHECKSEQUENCEVERIFY DROP DUP HASH160 <pubKeyHash> EQUALVERIFY CHECKSIG

具有條件控制的腳本(Conditional Clauses)

- if (condition):
- code to run when condition is true
- else:
- code to run when condition is false
- code to run in either case

- condition
- IF
- code to run when condition is true
- ELSE
- code to run when condition is false
- ENDIF
- code to run in either case

Locking script

IF

<Alice's Pubkey> CHECKSIG

ELSE

<Bob's Pubkey> CHECKSIG

ENDIF

Unlocking script

<Alice's Sig> 1 or <Bob's Sig> 0

Median Time Past (MTP)(BIP-113)

Block	Timestamp	MTP	MTP-6	Diff	Difficulty Adjust?
478582	Aug 2, 2017 11:36:31 AM	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 10:15:01 PM	13:21:30	Yes
478581	Aug 2, 2017 11:36:31 AM	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 9:51:49 PM	13:44:42	Yes
478580	Aug 2, 2017 11:36:31 AM	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 8:07:01 PM	15:29:30	Yes
478579	Aug 2, 2017 11:36:31 AM	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 6:38:29 PM	16:58:02	Yes
478578	Aug 2, 2017 11:36:31 AM	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 4:39:21 PM	18:57:10	Yes
478577	Aug 2, 2017 11:36:31 AM	Aug 2, 2017 11:20:19 AM	Aug 1, 2017 4:35:44 PM	18:44:35	Yes
478576	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 10:15:01 PM	Aug 1, 2017 4:05:15 PM	6:09:46	No
478575	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 9:51:49 PM	Aug 1, 2017 2:37:44 PM	7:14:05	No
478574	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 8:07:01 PM	Aug 1, 2017 1:52:58 PM	6:14:03	No
478573	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 6:38:29 PM	Aug 1, 2017 1:37:19 PM	5:01:10	No
478572	Aug 2, 2017 11:36:31 AM	Aug 1, 2017 4:39:21 PM	Aug 1, 2017 1:33:06 PM	3:06:15	No
478571	Aug 2, 2017 11:20:19 AM	Aug 1, 2017 4:35:44 PM	Aug 1, 2017 1:12:41 PM	3:23:03	No
478570	Aug 1, 2017 10:15:01 PM	Aug 1, 2017 4:05:15 PM	Aug 1, 2017 8:16:14 AM	7:49:01	No
478569	Aug 1, 2017 9:51:49 PM	Aug 1, 2017 2:37:44 PM	Aug 1, 2017 8:11:24 AM	6:26:20	No
478568	Aug 1, 2017 8:07:01 PM	Aug 1, 2017 1:52:58 PM	Aug 1, 2017 8:09:41 AM	5:43:17	No
478567	Aug 1, 2017 6:38:29 PM	Aug 1, 2017 1:37:19 PM	Aug 1, 2017 8:08:34 AM	5:28:45	No
478566	Aug 1, 2017 4:39:21 PM	Aug 1, 2017 1:33:06 PM	Aug 1, 2017 8:07:27 AM	5:25:39	No
478565	Aug 1, 2017 4:35:44 PM	Aug 1, 2017 1:12:41 PM	Aug 1, 2017 7:37:28 AM	5:35:13	No
478564	Aug 1, 2017 4:05:15 PM	Aug 1, 2017 8:16:14 AM	Aug 1, 2017 7:16:09 AM	1:00:05	No
478563	Aug 1, 2017 2:37:44 PM	Aug 1, 2017 8:11:24 AM	Aug 1, 2017 6:35:49 AM	1:35:35	No
478562	Aug 1, 2017 1:52:58 PM	Aug 1, 2017 8:09:41 AM	Aug 1, 2017 6:32:21 AM	1:37:20	No
478561	Aug 1, 2017 1:37:19 PM	Aug 1, 2017 8:08:34 AM	Aug 1, 2017 6:17:26 AM	1:51:08	No
478560	Aug 1, 2017 1:33:06 PM	Aug 1, 2017 8:07:27 AM	Aug 1, 2017 6:06:15 AM	2:01:12	No
478559	Aug 1, 2017 1:12:41 PM	Aug 1, 2017 7:37:28 AM	Aug 1, 2017 5:56:52 AM	1:40:36	No
478558	Aug 1, 2017 8:16:14 AM	Aug 1, 2017 7:16:09 AM	Aug 1, 2017 5:36:48 AM	1:39:21	No