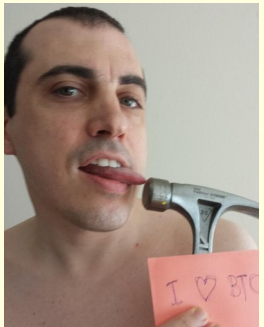
From shiba to lion

CRYPTO LYON

MERCI ANDREAS ANTONOPOULOS



CRYPTO LYON

Le sujet de la présentation

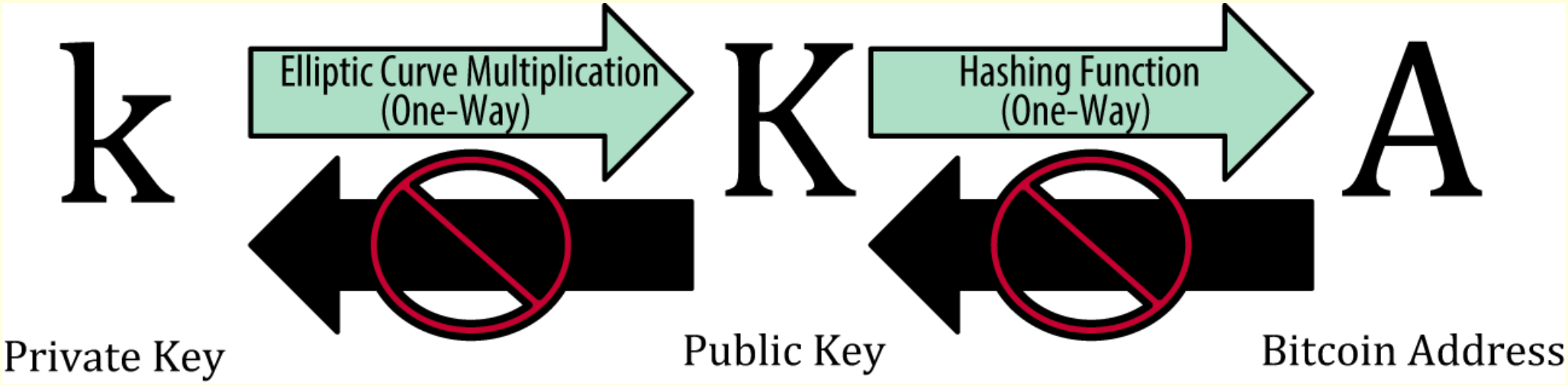
- Les clefs et adresses.
- Commment ?
- Les formats
- Le chiffrement (BIP38)

CRYPTO LYON

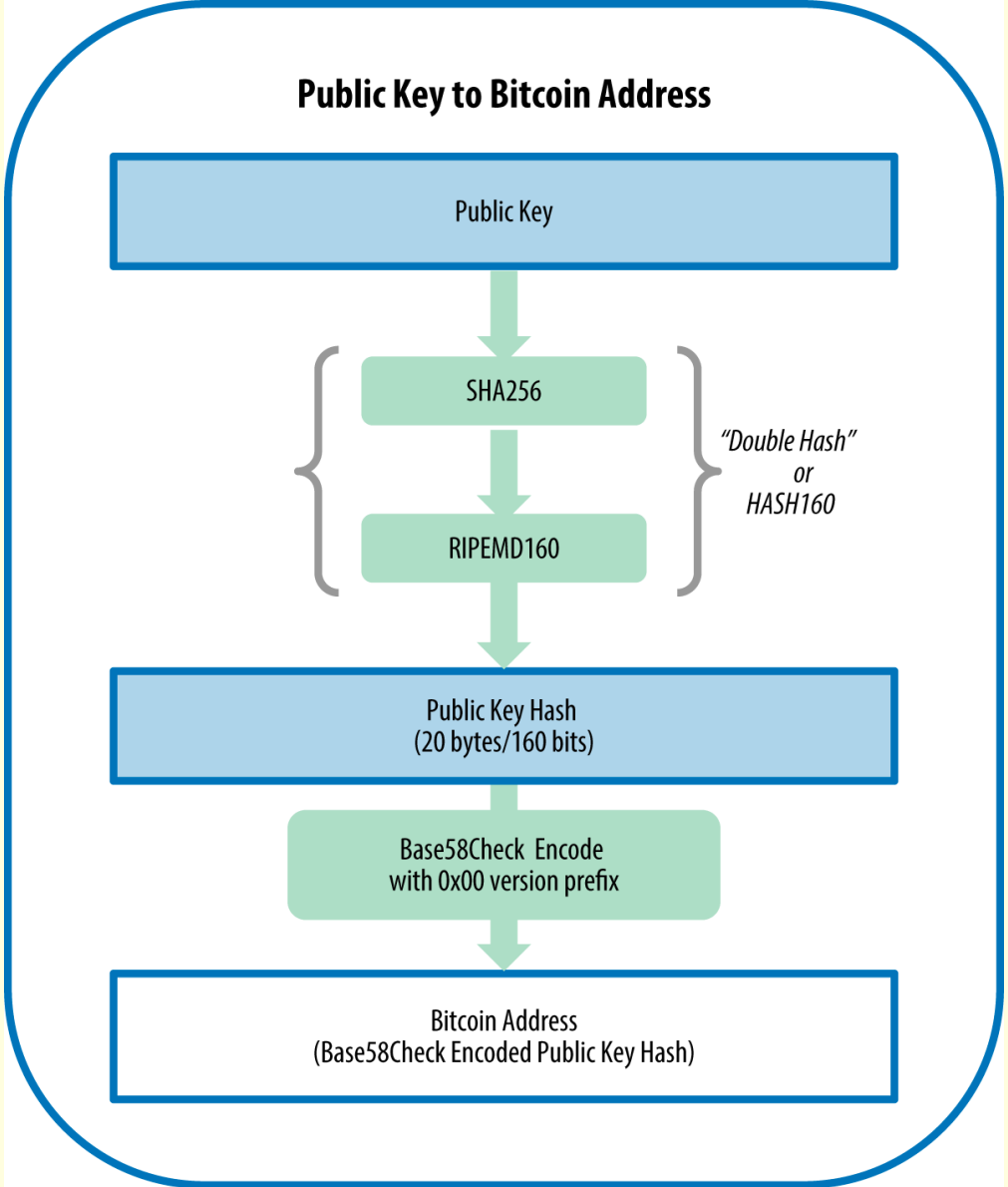
Des clefs, une addresse

- Une clef privée => un nombre random
- Une clef publique => un point sur une courbe * la clef privée
- Une addresse => Un hash (+ un checksum) de la clef publique

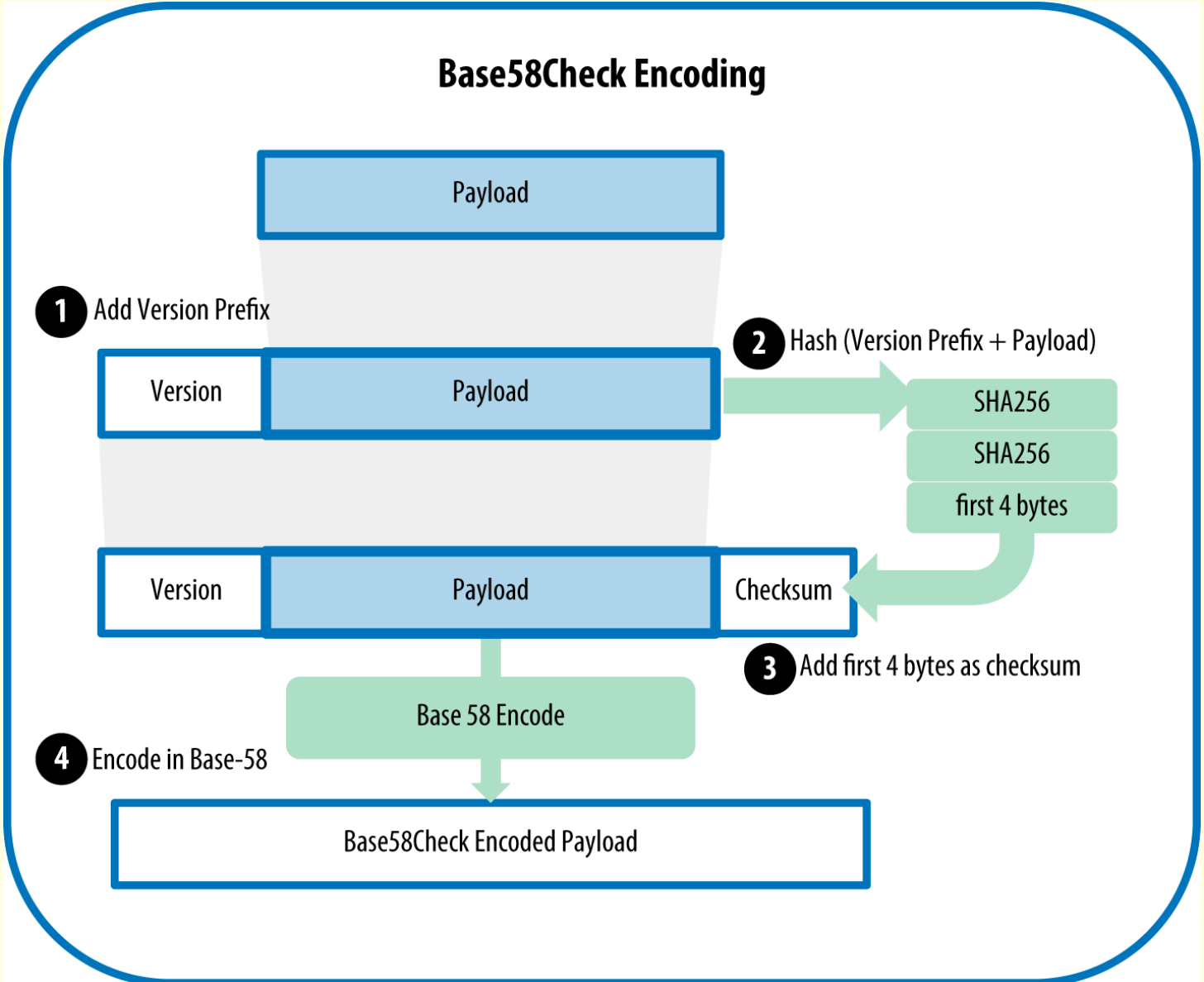
CRYPTO LYON


k
Elliptic Curve Multiplication
(One-Way)
K
Hashing Function
(One-Way)
A
Private Key
Public Key
Bitcoin Address

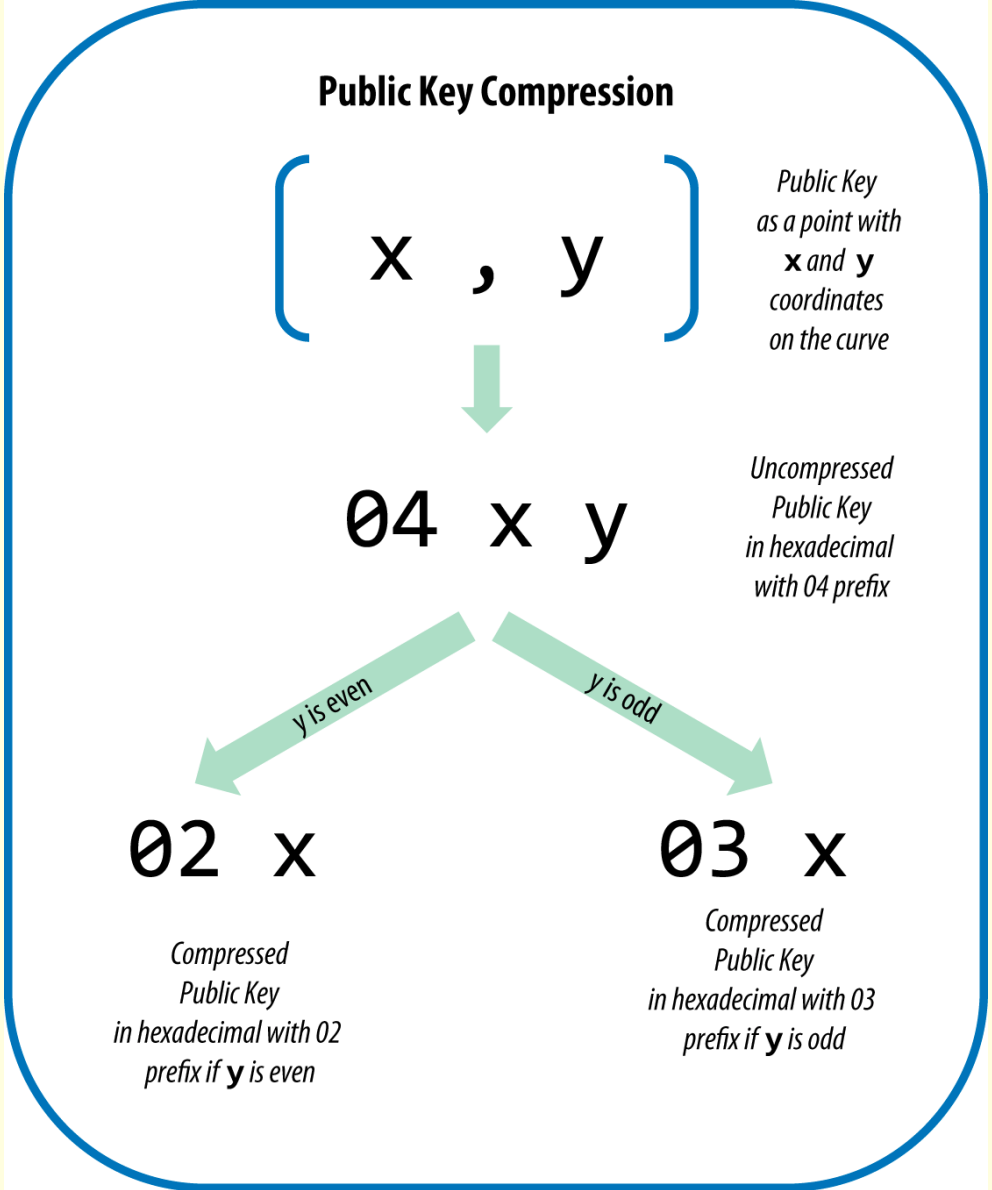
CRYPTO LYON


Public Key to Bitcoin Address
Public Key
SHA256
RIPEMD160
"Double Hash"
or
HASH160
Public Key Hash
(20 bytes/160 bits)
Base58Check Encode
with 0x00 version prefix
Bitcoin Address
(Base58Check Encoded Public Key Hash)

CRYPTO LYON

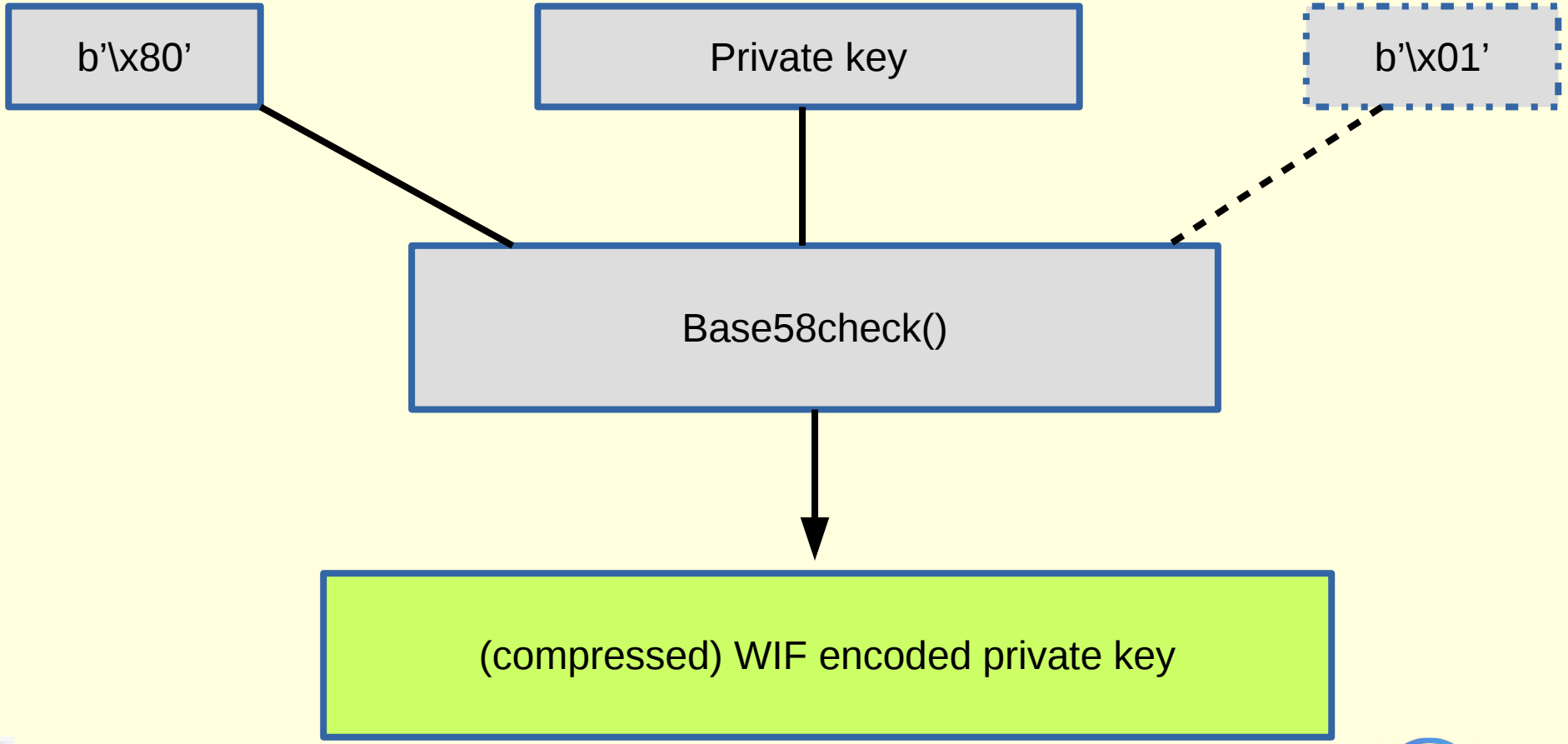

Base58Check Encoding
Payload
1 Add Version Prefix
Version
Payload
2 Hash (Version Prefix + Payload)
SHA256
SHA256
first 4 bytes
Version
Payload
Checksum
3 Add first 4 bytes as checksum
Base 58 Encode
4 Encode in Base-58
Base58Check Encoded Payload

CRYPTO LYON


Public Key Compression
[x , y]
Public Key as a point with x and y coordinates on the curve
04 x y
Uncompressed Public Key in hexadecimal with 04 prefix
y is even
y is odd
02 x
Compressed Public Key in hexadecimal with 02 prefix if y is even
03 x
Compressed Public Key in hexadecimal with 03 prefix if y is odd

CRYPTO LYON

Wallet Import Format



CRYPTO LYON

Table 1. Base58Check version prefix and encoded result examples

Type	Version prefix (hex)	Base58 result prefix
Bitcoin Address	0x00	1
Pay-to-Script-Hash Address	0x05	3
Bitcoin Testnet Address	0x6F	m or n
Private Key WIF	0x80	5, K, or L
BIP-38 Encrypted Private Key	0x0142	6P
BIP-32 Extended Public Key	0x0488B21E	xpub

Table 4. Example: Same key, different formats

Format	Private key
Hex	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
WIF	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
Hex-compressed	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD01
WIF-compressed	KxFC1jmwwCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrtJ

Table 5. Example of BIP-38 encrypted private key

Private Key (WIF)	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
Passphrase	MyTestPassphrase
Encrypted Key (BIP-38)	6PRTHL6mWa48xSopbU1cKrVjpKbBZxcLRRCdctLJ3z5yxE87MobKoXdTsJ

CRYPTO LYON