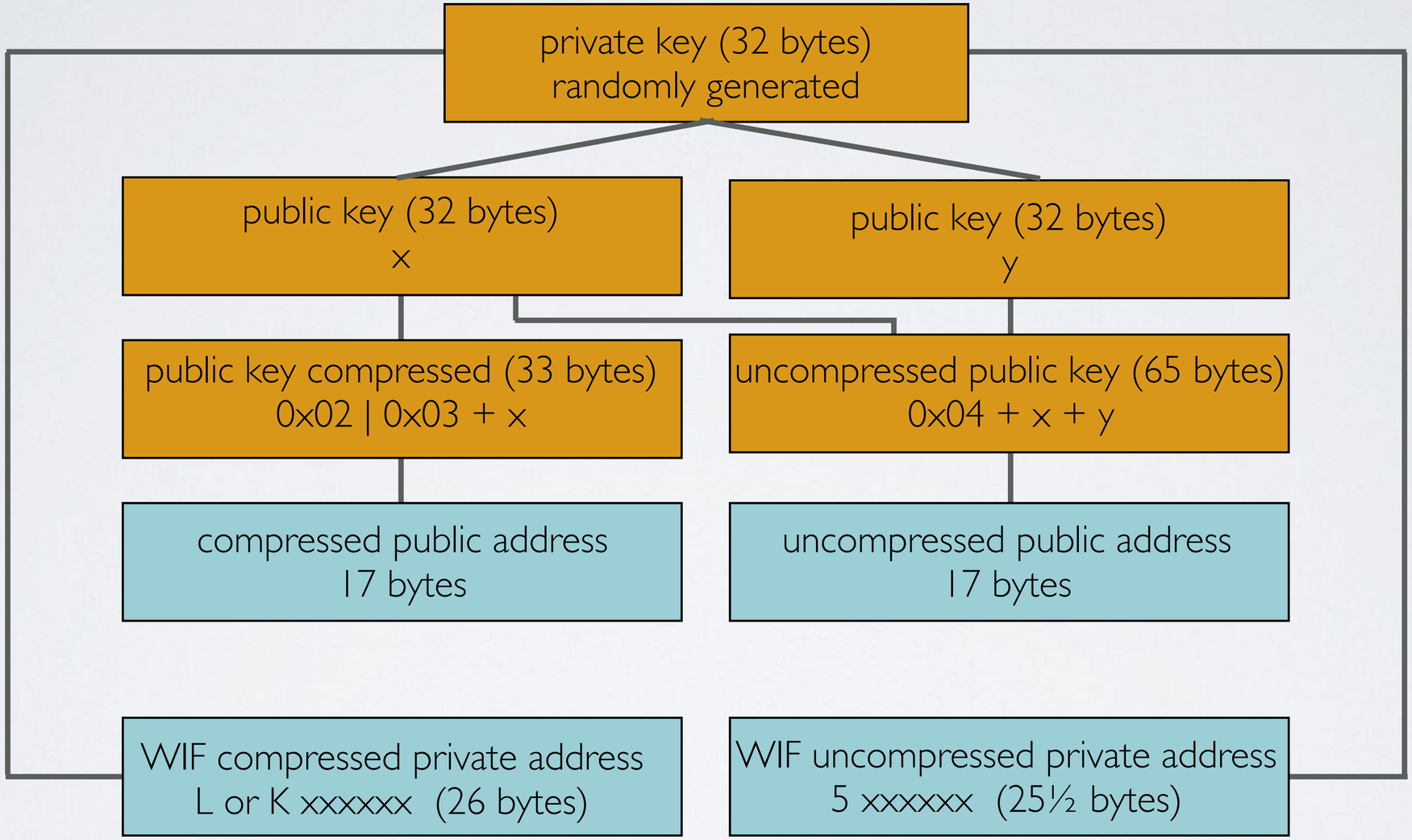
BLOCKCHAIN TUTORIAL 16

Bitcoin compressed and uncompressed addresses

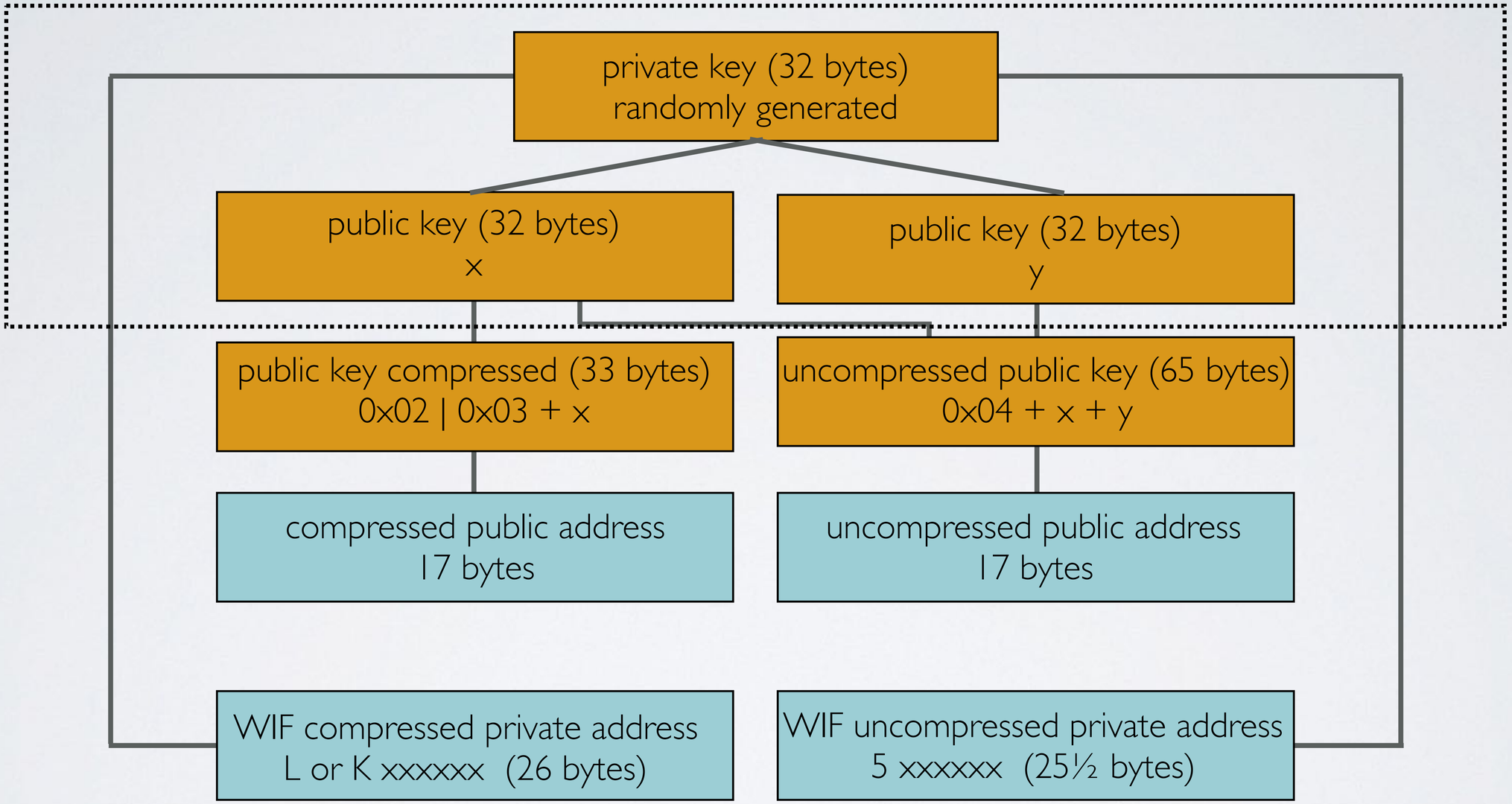
BLOCKCHAIN TUTORIAL 16

Bitcoin compressed and uncompressed addresses

BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



BITCOIN PRIVATE AND PUBLIC KEY

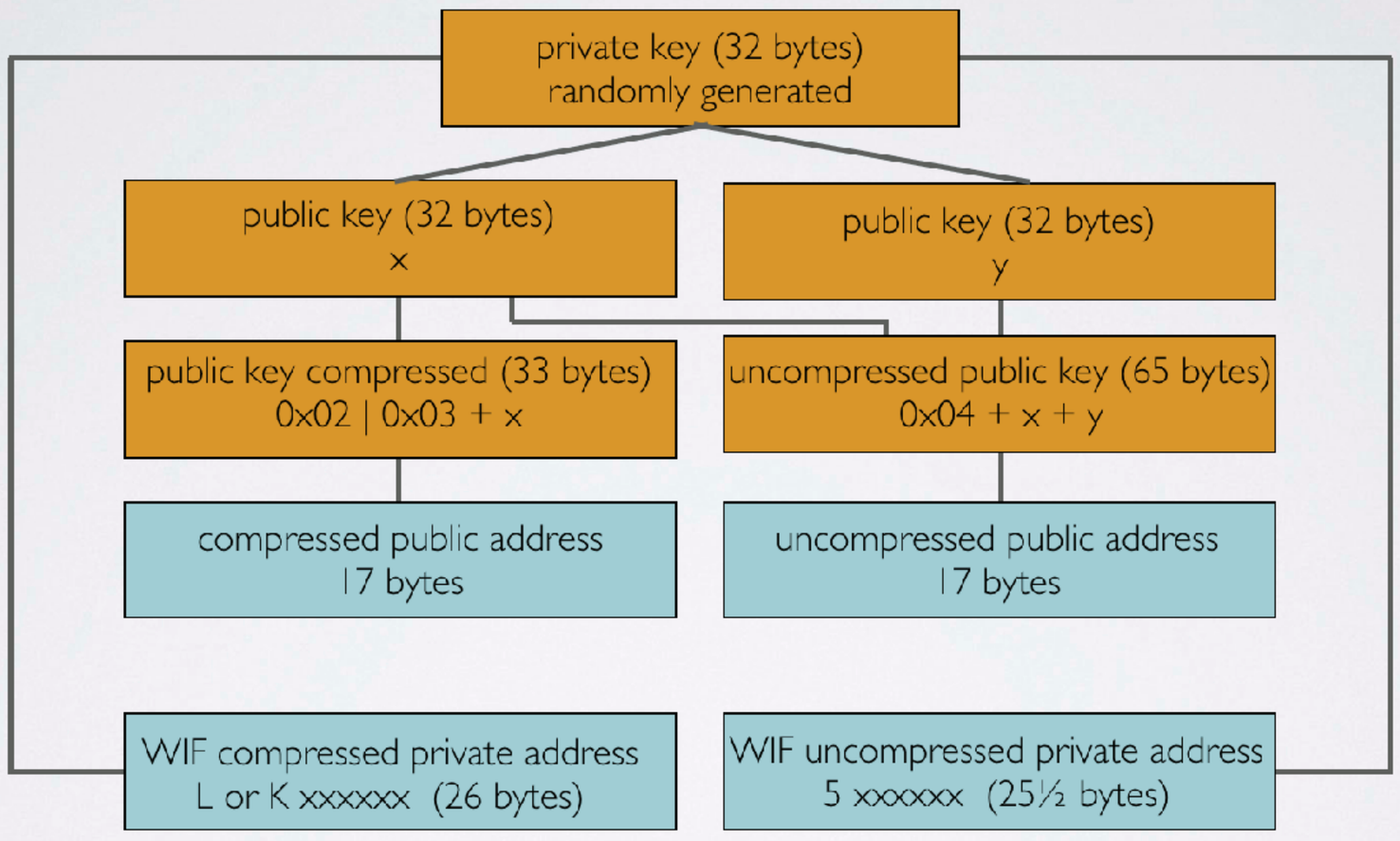
- By now you should know that a randomly generated number is the private key and this key is used to calculate the public key which is a pair of integers(x, y)

Private key hex (32 bytes):
0x79FE45D6133918I238E49424E905446A35497A8ADEA8B7D5241A1E7F2C95A04D

Public key x-value (32 bytes):
0x2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872

Public key y-value (32 bytes):
0x0336C5EB647E891C98261C57C13098FA6AE68221363C68FF15841B86DAD60241

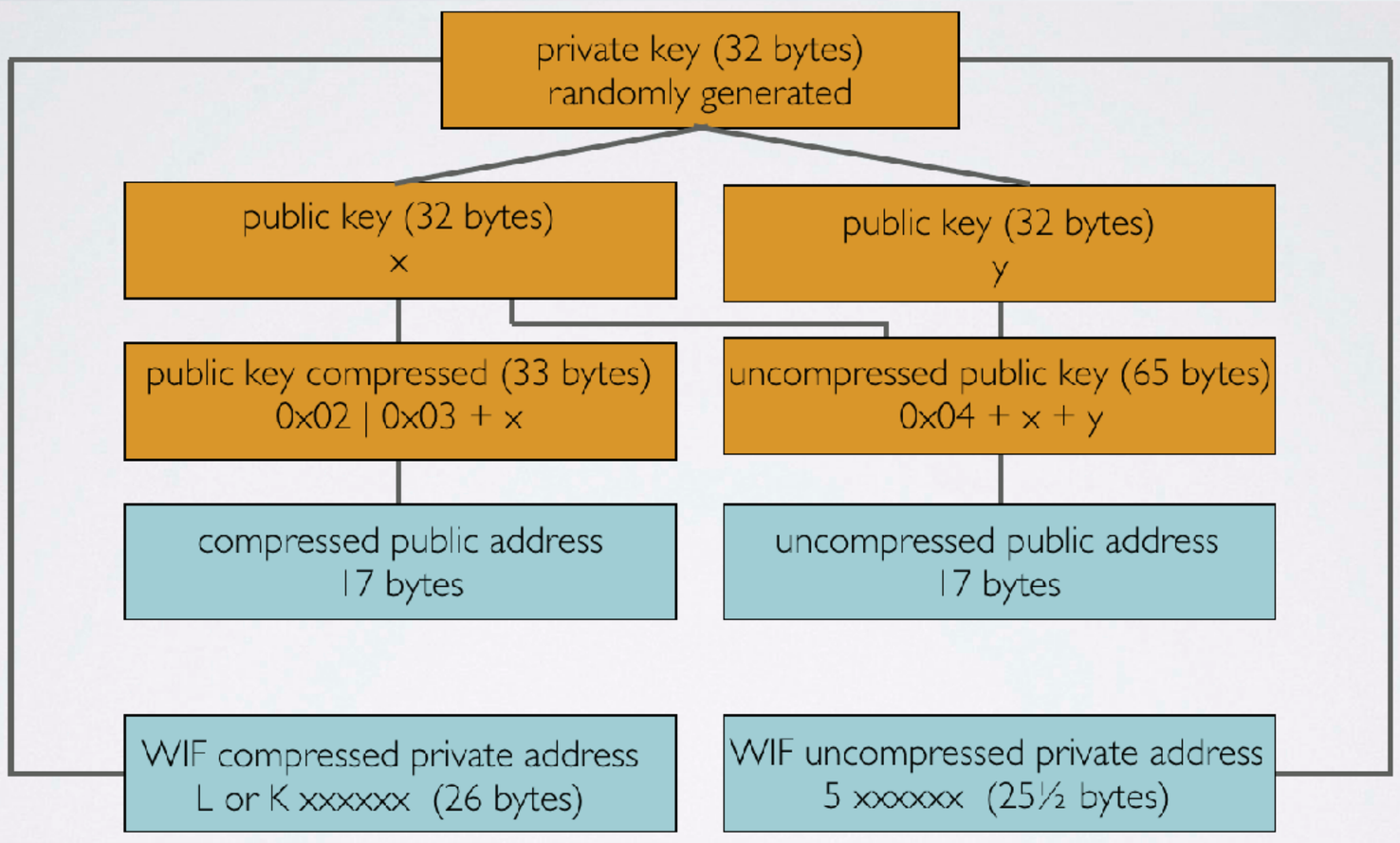
BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



There are 2 methods for using the private key to generate 2 different public keys and thus 2 different public addresses.

One method will generate a compressed public key (33 bytes) and the other an uncompressed public key (65 bytes).

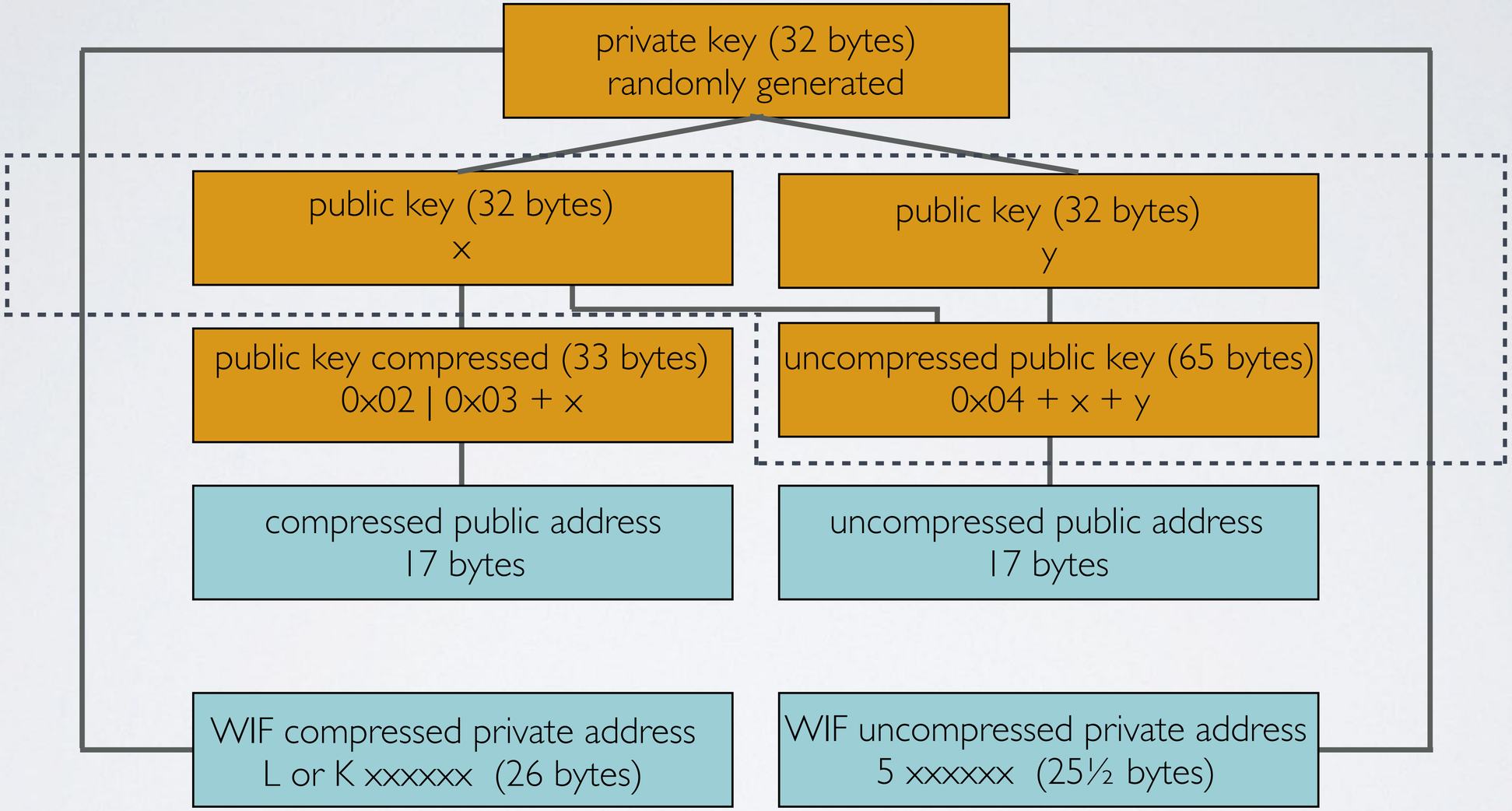
BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



Some Bitcoin clients (software program) can work with both compressed an uncompressed public keys and some clients can only work with one type.

The private key is converted in such a way which tells Bitcoin clients how to interpret the private key and which version of the public key/address to generate when importing.

BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



BITCOIN UNCOMPRESSED PUBLIC KEY

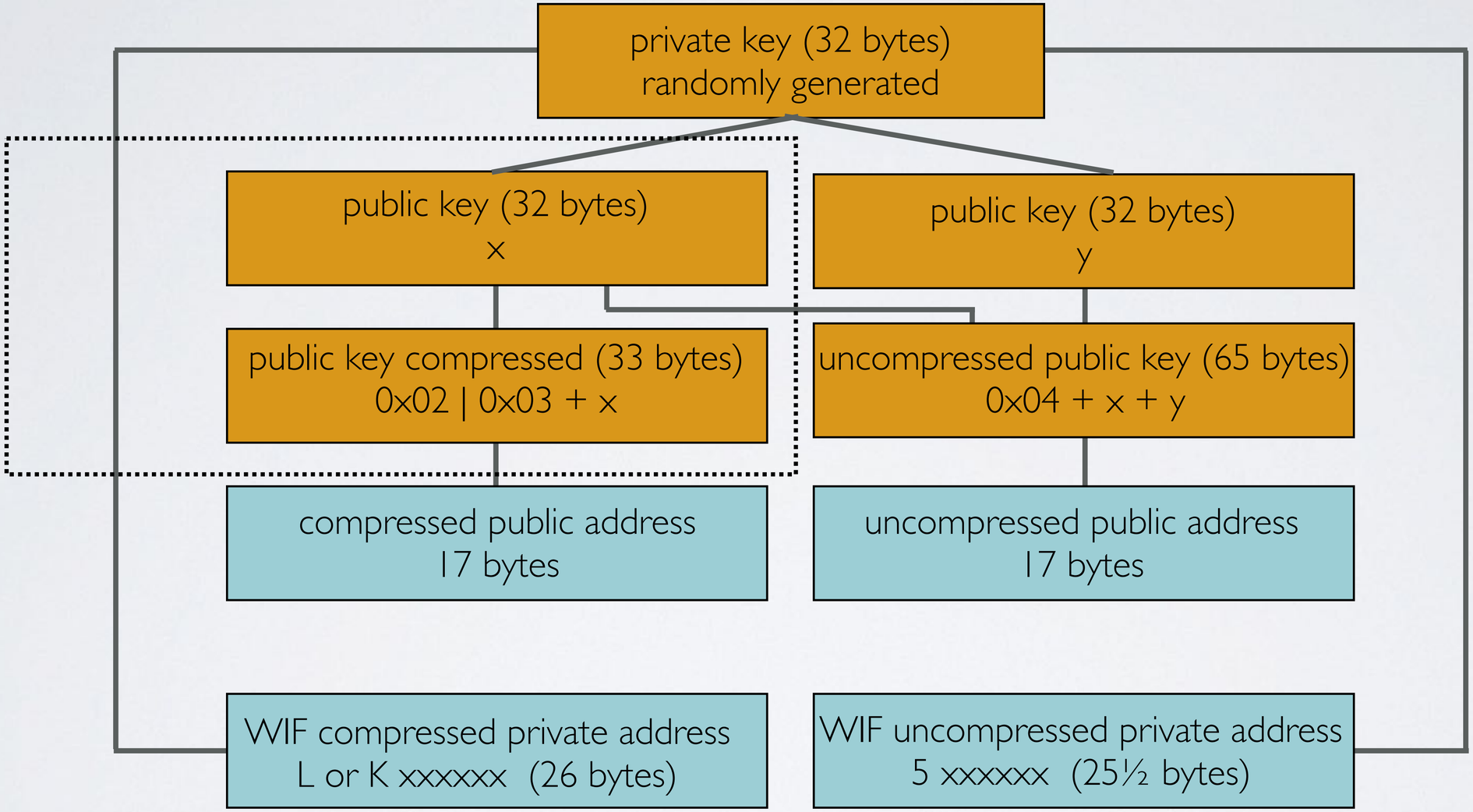
- For Bitcoin uncompressed public keys the x and y values, both 32 bytes long, are concatenated together, and then prepended with a single 0x04 byte.

Public key x-value (32 bytes):
0x2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872

Public key y-value (32 bytes):
0x0336C5EB647E891C98261C57C13098FA6AE68221363C68FF15841B86DAD60241

Uncompressed public key: 0x04 + x + y (1 + 32 + 32 = 65 bytes):
0x04 2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872
0336C5EB647E891C98261C57C13098FA6AE68221363C68FF15841B86DAD60241

BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



BITCOIN COMPRESSED PUBLIC KEY

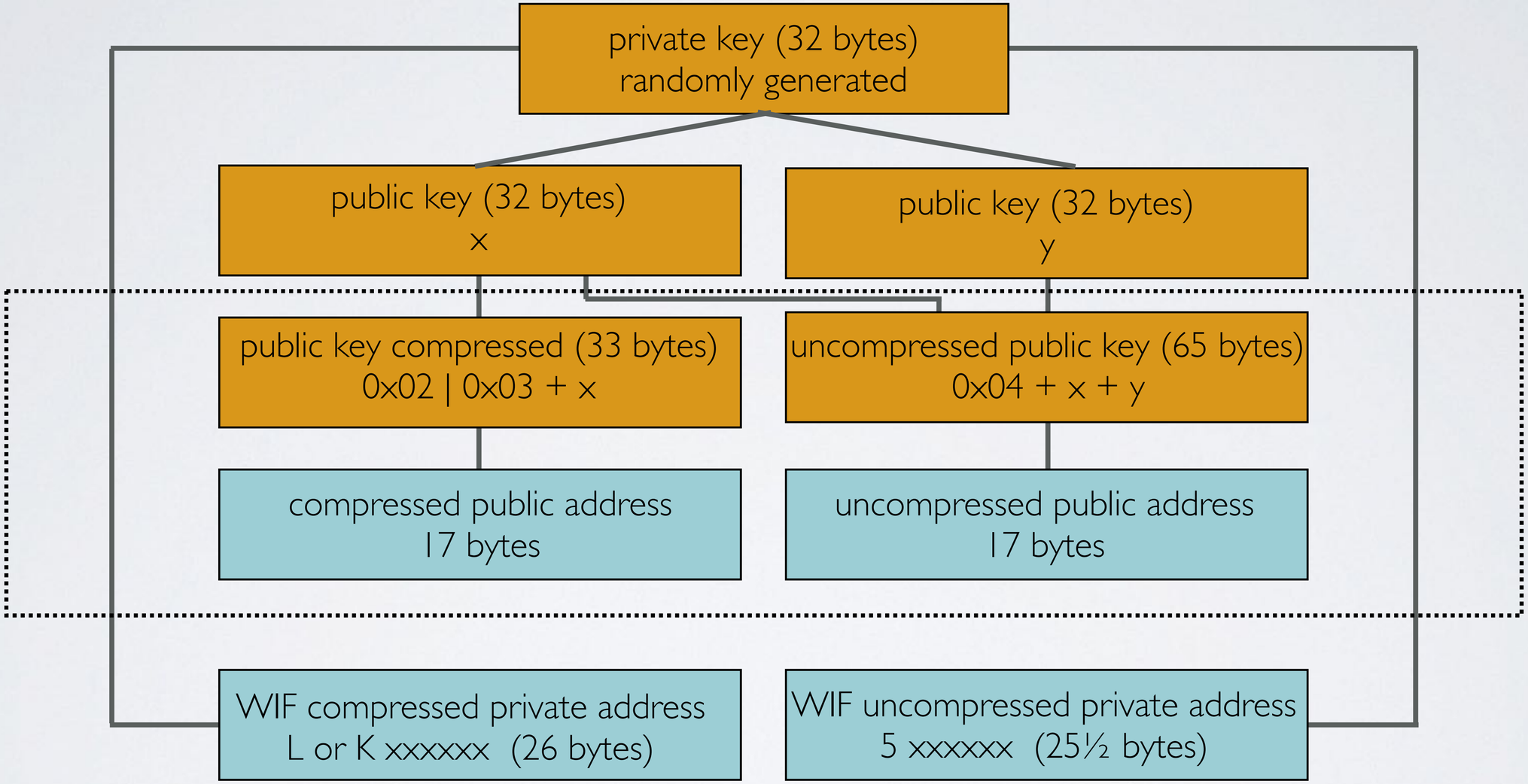
- For Bitcoin compressed public keys a single 0x02 or 0x03 byte is prepended on the x values. Which of these two single bytes is used depends on the y value. Prepend 0x02 if the y value is even and 0x03 if the y value is odd.

Public key x-value (32 bytes):
0x2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872

Public key y-value (32 bytes):
0x0336C5EB647E891C98261C57C13098FA6AE68221363C68FF15841B86DAD60241

Compressed public key: 0x03 + x (1 + 32 = 33 bytes):
0x03 2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872

BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



BITCOIN (UN)COMPRESSED PUBLIC ADDRESSES

- Bitcoin uncompressed and compressed public keys result in different addresses, but they still come from the same private key.

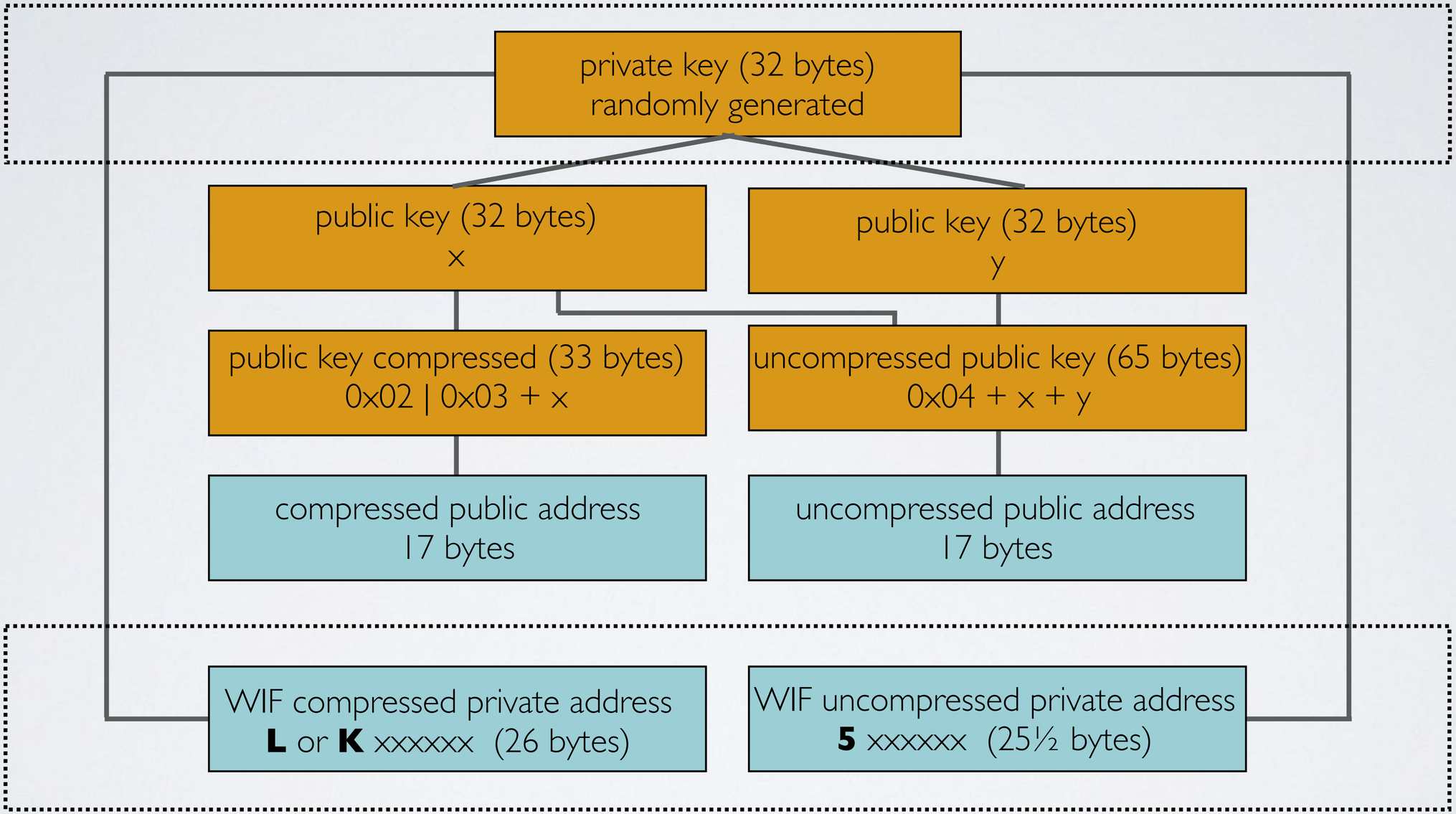
Uncompressed public key (65 bytes):
0x04 2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872
0336C5EB647E891C98261C57C13098FA6AE68221363C68FF15841B86DAD60241

Uncompressed public address (17 bytes):
1P6LTFY9TMMJNQMNRAV4DBCV6274DDATIR

Compressed public key (33 bytes):
0x03 2A574EA59CAE80B09D6BA415746E9B031ABFBE83F149B43B37BE035B87164872

Compressed public address (17 bytes):
1ADS8LK6VN87RI9HFJOFDUPLNO76CWQUMF

BITCOIN (UN)COMPRESSED PRIV PUB ADDRESSES



BITCOIN (UN)COMPRESSED PRIVATE ADDRESSES

- Usually a private key in WIF (**W**allet **I**mport **F**ormat) has a different prefix to tell the wallet whether it should handle the key as one for a compress or an uncompressed address.

Private key hex (32 bytes):
0x79FE45D6133918I238E49424E905446A35497A8ADEA8B7D5241A1E7F2C95A04D

Uncompressed private address (51 chars, 25½ bytes):
5JK1JCETE58MZYXA9ZYFXBGRBVXHXEAHYHEXF5WWKPAGFDVHAWD

Compressed private address (52 chars, 26 bytes):
L1JRF4WNKHDVEZ87QGXW6CK5ZGPQTGSMQSWWQ8W8K8QIFXZTAPQF

- Bitcoin uncompressed private addresses begins with the character 5 and compressed private addresses begins with the character L or K.

ADDITIONAL INFORMATION

- If the compressed public address is needed the private key starts with K or L, if the uncompressed public address is needed the private key will start with 5.

- Bitcoin clients can only receive coins on compressed addresses if they support compressed public keys in the first place.

- The advantage of using compressed public keys is smaller transactions on the network and smaller blockchain sizes. A compressed public key has only 33 bytes instead of 65 bytes.

- The standard Bitcoin client version 0.6 has introduced compressed keys.