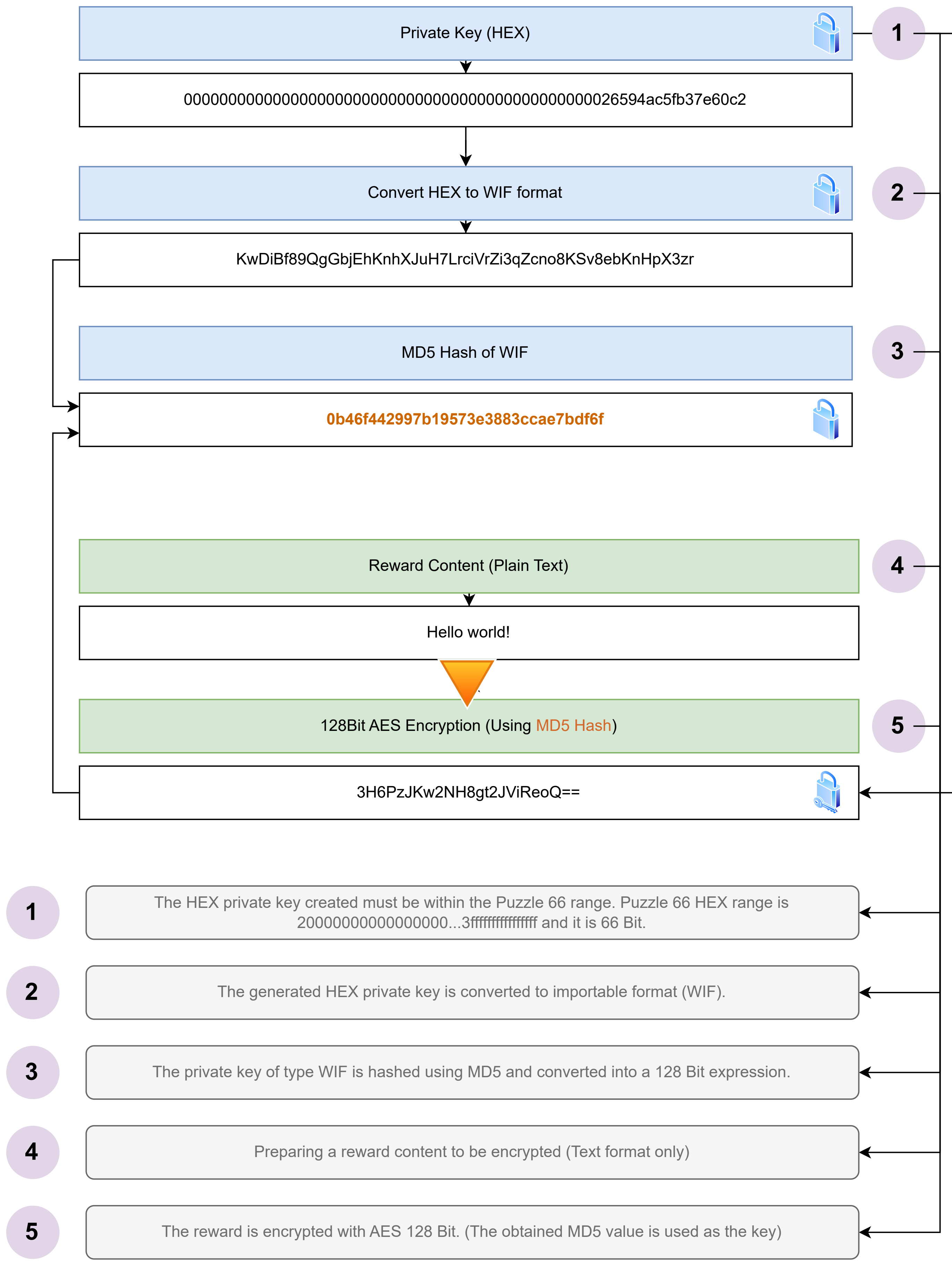
Reward creation example (Puzzle 66)



1 Private Key (HEX)

00000000000000000000000000000000000000000000000026594ac5fb37e60c2

2 Convert HEX to WIF format

KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qZcno8KSv8ebKnHpX3zr

3 MD5 Hash of WIF

0b46f442997b19573e3883ccae7bdf6f

4 Reward Content (Plain Text)

Hello world!

5 128Bit AES Encryption (Using MD5 Hash)

3H6PzJKw2NH8gt2JViReoQ==

1 The HEX private key created must be within the Puzzle 66 range. Puzzle 66 HEX range is 20000000000000000...3ffffffffffffffff and it is 66 Bit.

2 The generated HEX private key is converted to importable format (WIF).

3 The private key of type WIF is hashed using MD5 and converted into a 128 Bit expression.

4 Preparing a reward content to be encrypted (Text format only)

5 The reward is encrypted with AES 128 Bit. (The obtained MD5 value is used as the key)

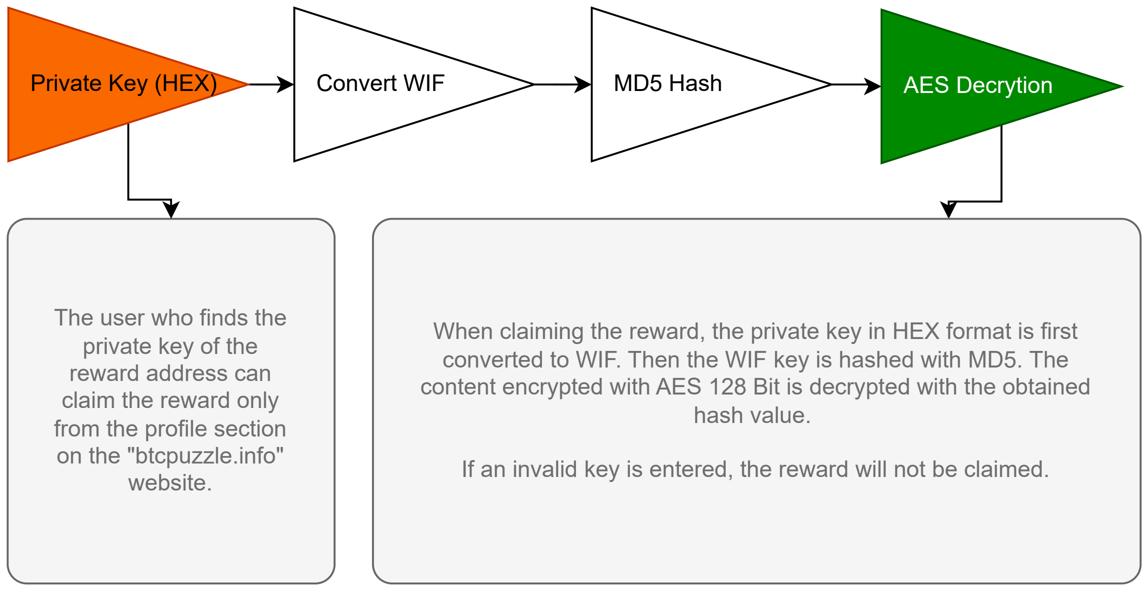
Other notes about rewards

Wallet Address (Reward Address)

1NRHE28Nzq1Mv6hm1ySa4eCVMf674tCVwW

According to the example on the left; The reward address will be above. Users will try to find the private key of this address. The chance of finding it is the same as solving the Puzzle 66.

Claim reward



The user who finds the private key of the reward address can claim the reward only from the profile section on the "btcpuzzle.info" website.

When claiming the reward, the private key in HEX format is first converted to WIF. Then the WIF key is hashed with MD5. The content encrypted with AES 128 Bit is decrypted with the obtained hash value.

If an invalid key is entered, the reward will not be claimed.

Encrypted reward content is known to btcpuzzle.info. The person who will claim the reward must scan the relevant range. Only the person who scans the relevant range can claim the reward.

In the Bitcrackrandomiser application, the private key of the reward address will be found in HEX format. WIF and MD5 hashing is done automatically by the system when claiming the reward.

BTCPUZZLE

https://btcpuzzle.info/

https://github.com/ilkerccom/bitcrackrandomiser

🔒 It is known only to the user who created the reward.

🔒 It is only known by the user who created the reward and btcpuzzle.info

🔓 It is known to everyone.

In the example above, Puzzle 66 is used as an example. For other puzzles, the only thing that will change will be the range. Pool rewards can only be claimed via the "btcpuzzle.info" website and the claiming user must have completed a minimum of 100 range scans. If a pool prize is not found, it can be removed by the user who created the prize by notifying btcpuzzle.info. (When the relevant puzzle is solved). Reward content is in text format only. Rewards can be created offline on the "btcpuzzle.info" website or in open source software.