CRYPTONOTE STANDARD 005 Albert Werner
Category: Main Track Montag
Prometheus
Tereno
CryptoNote
October 2012

CryptoNote Transaction Extra Field

Abstract

This document is part of the CryptoNote Standards describing a peer-to-peer anonymous payment system. It defines the way extra data can be added to a CryptoNote transaction. The content of transaction Extra field is not verified by the network. Transaction Extra field can contain arbitrary data.

Copyright and License Notice

Table of Contents

1. Introduction

Every transaction contains the Extra field, which is a part of transaction prefix (i.e. is signed) [CNS004].

All network nodes verify CryptoNote transactions before they are included into blocks. If verification fails, a transaction will be rejected. However, the content of Extra field is not verified.

2. Definitions

transaction: a single record of assets ownership transfer

transaction prefix: the part of a transaction that contains all the data except signatures

3. Extra Field Format

The value of Extra field is an array of bytes. In transactions, the array is preceded by its size value:

```
+------------+-------------------------+
|  Size      |  Transaction Extra data  |
|  (varint)  |  (array of bytes)        |
+------------+-------------------------+
```

Figure 3a: Extra field size

The Extra field can be used to store certain user-defined content.

There are common rules for the interpretation of the content of Extra field to ensure compatibility among different software.

The Extra field can contain several sub-fields. Each sub-field contains a sub-field tag followed by sub-field content. The sub-field tag indicates the nature of the data. In some cases the size of the data is implied by the sub-field tag itself (Figure 3b). In other cases the size is specified explicitly after the sub-field tag (Figure 3c). The list of the defined sub-field tags is provided in the next section.

```
+-------+--------+
|  Tag  |  Data  |
+-------+--------+
```

Figure 3b: Data size implied by the sub-field tag

```
+-------+--------+--------+
|  Tag  |  Size  |  Data  |
+-------+--------+--------+
```

Figure 3c: Data size specified explicitly

If the data size is specified explicitly, it is encoded as varint (variable-length encoding of integers). See section 3 of [CNS003].

4. Sub-Field Tags

This section defines known sub-fields tags and the corresponding data sizes. If the size is missing in this table, it has to be explicitly specified as shown in Figure 3c.

Value	Length	Meaning
0x00	-	Transaction padding. The following restrictions apply: - padding is allowed only at the end of the Extra field, - padding can only contain null bytes, - the padding length is limited to 255 bytes, - no explicit size is specified for padding (it occupies the remaining space of the Extra field)
0x01	32 bytes	Transaction public key
0x02	-	Extra nonce (for pooled mining)

Table 4: Sub-field tag descriptions

5. Example

Below is an example of Extra field of a base transaction with three sub-fields:

- transaction public key (size is omitted for the public key; it always equals 32 bytes),

- extra nonce (size is specified explicitly),

- transaction padding (size is omitted; only null bytes are possible).

```
+--------------------+--------+
|  Extra field size  |  0x78  |
+--------------------+--------+

+--------------------+--------+-----------------------+
|  Tx public key     |  0x01  |  32-byte public key   |
+--------------------+--------+-----------------------+
                        Tag      Data

+--------------------+--------+--------+-------------+
|  Extra nonce       |  0x02  |  0x52  |  . . . . .  |
+--------------------+--------+--------+-------------+
                        Tag      Size     Data

+--------------------+--------+-------------+
|  Tx size padding   |  0x00  |  0x00 0x00  |
+--------------------+--------+-------------+
                        Tag      Data
```

Figure 5: Transaction Extra field example

6. References

[CNS003] "CryptoNote Blockchain", CryptoNote Standard 003, September 2012.

[CNS004] "CryptoNote Transactions", CryptoNote Standard 004, September 2012.