

## Appendix A: DMeta Hash Contract – Creating Contracts using Hash Values

- <https://godmeta.github.io/dmcontract/>

DMetaContract: Decentralized Meta Contract

DMetaHash: Base64 53-bit Hash

Contract to hash:

Brian will transfer USD50 to Trinity, via local banks, after Adam sends TRX-USDT50 to Brian.

DMetaHash

DMetaHash of Contract:

A+stdDVniQ==

DMC3 Triplets:

A+stdDVniQ== ERzUEXhTIQ== HqglWae13Q==

DMC3

ROOT

Root Hash (Hash of All Hashes):

BVJPGujiGg==

Decentralized Meta Contract (DMetaContract, DMC) is arguably the simplest smart contract ever invented.

Figure 1

In DMeta Hash Contract example above, the contract text is:

- Brian will transfer USD50 to Trinity, via local banks, after Adam sends TRX-USDT50 to Brian.

The corresponding Contract Hash is A+stdDVniQ== .

The hashes of the signing parties are ERzUEXhTIQ== and HqglWae13Q== .

The root hash (hash of the contract hash and hashes of signatories) is BVJPGujiGg== .

### DMeta Transaction

For the convenience of discussions, let us define a “transaction” as a series of contracts. This definition may sound counterintuitive to conventional understanding. Let us elaborate and explain using some examples:

1. Adam asked Brian to buy a cup of coffee from a Starbuck’s down the street.
2. Brian went to the Starbuck’s, bought a cup of coffee, brought it to Adam, and collected RM20 from Adam.
3. (1) and (2) can be considered as one “transaction” in the conventional sense.

4. Consider translating the above events into DMeta Hash Contracts (DHC):

A. (1) becomes a DHC where the contract text is:

- Adam asked Brian to buy a cup of coffee from a Starbuck's down the street.

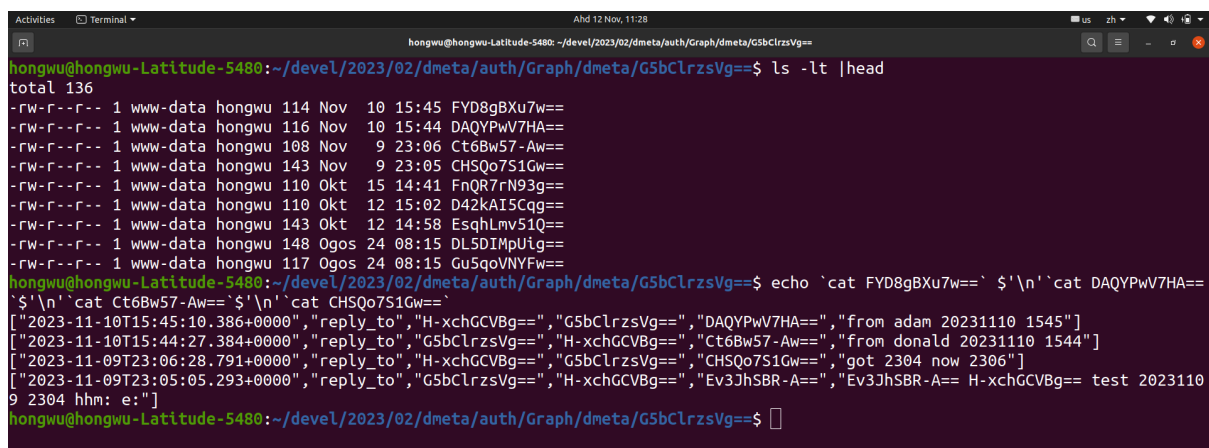
B. (2) becomes 2 DHC where the contract texts are:

- i. Brian went to the Starbuck's, bought a cup of coffee, brought it to Adam.
- ii. Brian collected RM20 from Adam.

In the following examples, 2 parties, with public key hashes being H-xchGCVBg== (adam) and G5bClrzsVg== (donald) respectively.

"ls -lt" lists the files in the subdirectory belonging to G5bClrzsVg== (donald) in reverse chronological order. Each file is a DMeta Hash Contract, where the filename is the root hash. The last 4 files concerned are:

1. FYD8gBXu7w==
2. DAQYPwV7HA==
3. Ct6Bw57-Aw==
4. CHSQo7S1Gw==

A terminal window with a dark background and light text. The prompt is 'hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg=='. The first command is 'ls -lt | head', which lists the first five files in reverse chronological order. The second command is 'echo `cat FYD8gBXu7w==` \$'\n\'`cat DAQYPwV7HA==` \$'\n\'`cat Ct6Bw57-Aw==` \$'\n\'`cat CHSQo7S1Gw==`', which displays the content of the first four files. The output shows JSON-like contract data with timestamps, reply\_to fields, and various hashes.

```
hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg== $ ls -lt | head
total 136
-rw-r--r-- 1 www-data hongwu 114 Nov 10 15:45 FYD8gBXu7w==
-rw-r--r-- 1 www-data hongwu 116 Nov 10 15:44 DAQYPwV7HA==
-rw-r--r-- 1 www-data hongwu 108 Nov 9 23:06 Ct6Bw57-Aw==
-rw-r--r-- 1 www-data hongwu 143 Nov 9 23:05 CHSQo7S1Gw==
-rw-r--r-- 1 www-data hongwu 110 Okt 15 14:41 FnQR7rN93g==
-rw-r--r-- 1 www-data hongwu 110 Okt 12 15:02 D42kA1SCqg==
-rw-r--r-- 1 www-data hongwu 143 Okt 12 14:58 EsqhLmv51Q==
-rw-r--r-- 1 www-data hongwu 148 Ogos 24 08:15 DL5DIMPuIg==
-rw-r--r-- 1 www-data hongwu 117 Ogos 24 08:15 Gu5qoVNYFW==
hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg== $ echo `cat FYD8gBXu7w==` $'\n\'`cat DAQYPwV7HA==` $'\n\'`cat Ct6Bw57-Aw==` $'\n\'`cat CHSQo7S1Gw==`
["2023-11-10T15:45:10.386+0000","reply_to","H-xchGCVBg==","G5bClrzsVg==","DAQYPwV7HA==","from adam 20231110 1545"]
["2023-11-10T15:44:27.384+0000","reply_to","G5bClrzsVg==","H-xchGCVBg==","Ct6Bw57-Aw==","from donald 20231110 1544"]
["2023-11-09T23:06:28.791+0000","reply_to","H-xchGCVBg==","G5bClrzsVg==","CHSQo7S1Gw==","got 2304 now 2306"]
["2023-11-09T23:05:05.293+0000","reply_to","G5bClrzsVg==","H-xchGCVBg==","Ev3JhSBR-A==","Ev3JhSBR-A== H-xchGCVBg== test 20231109 2304 hhm: e:"]
hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg== $
```

Figure 2

Starting from the last file (first in reverse chronological order) FYD8gBXu7w== the contents are (figure 2):

["2023-11-10T15:45:10.386+0000","reply\_to","H-xchGCVBg==","G5bClrzsVg==","DAQYPwV7HA==","from adam 20231110 1545"]

```
hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg==$ ls -lt |head
total 136
-rw-r--r-- 1 www-data hongwu 114 Nov 10 15:45 FYD8gBXu7w==
-rw-r--r-- 1 www-data hongwu 116 Nov 10 15:44 DAQYPwV7HA==
-rw-r--r-- 1 www-data hongwu 108 Nov 9 23:06 Ct6Bw57-Aw==
-rw-r--r-- 1 www-data hongwu 143 Nov 9 23:05 CHSQo7S1Gw==
-rw-r--r-- 1 www-data hongwu 110 Okt 15 14:41 FnQR7rN93==
-rw-r--r-- 1 www-data hongwu 110 Okt 12 15:02 D42kAI5Cqg==
-rw-r--r-- 1 www-data hongwu 143 Okt 12 14:58 EsqhLmv51Q==
-rw-r--r-- 1 www-data hongwu 148 Ogos 24 08:15 DL5DIMpUig==
-rw-r--r-- 1 www-data hongwu 117 Ogos 24 08:15 Gu5qoVNYFW==
hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg==$ echo `cat FYD8gBXu7w==
`$'\n'`cat Ct6Bw57-Aw==`$'\n'`cat CHSQo7S1Gw==`
["2023-11-10T15:45:10.386+0000","reply_to","H-xchGCVBg==","G5bClrzsVg==","DAQYPwV7HA==","from adam 2023
["2023-11-10T15:44:27.384+0000","reply_to","G5bClrzsVg==","H-xchGCVBg==","Ct6Bw57-Aw==","from donald 20
["2023-11-09T23:06:28.791+0000","reply_to","H-xchGCVBg==","G5bClrzsVg==","CHSQo7S1Gw==","got 2304 now 2
["2023-11-09T23:05:05.293+0000","reply_to","G5bClrzsVg==","H-xchGCVBg==","Ev3Jh5BR-A==","Ev3Jh5BR-A== H
9 2304 hhm: e:"]
hongwu@hongwu-Latitude-5480:~/devel/2023/02/dmeta/auth/Graph/dmeta/G5bClrzsVg==$
```

Figure 3

The fields are (figure 3):

- i. timestamp
- ii. type
- iii. sender's hash (left yellow arrow)
- iv. recipient's hash (right yellow arrow)
- v. previous contract root hash. (red arrows)
- vi. contract text

In this example, the contents of the contract do not show much useful information other than the sender's name and time. However, it suffices to demonstrate a DMeta Transaction, consisting of a series of DMeta Hash Contracts, which embed the previous root hash in the current contract.