DigitalBits ERC20 Token Burn

Date: 26/11/2019
Revision after burn: 28/11/2019

Prepared for:
Al Burgio, Founder, DigitalBits
Michael Lukchoo, VP of Operations, DigitalBits

Prepared by:
Martin Derka, PhD, Senior Research Engineer, Quantstamp
Alex Murashkin, MMath, Senior Software Engineer, Quantstamp

1. Executive Summary

The DigitalBits token referenced herein is an ERC20 token with ticker XDB and address 0xb9eefc4b0d472a44be93970254df4f4016569d27 on both Ethereum Mainnet and Ropsten. The total supply of the token is 100,000,000,000 (excluding 7 decimals) at block #9004707 (see section 4 for details). The token is burnable. DigitalBits team would like to reduce the total supply to 1,500,000,000 by burning 98,500,000,000 XDB ERC20 tokens that are currently in possession of the team under 8 different accounts.

This report is prepared by Quantstamp Inc. to assist with burning the tokens and to justify the events.

2. Approach and Methodology

A single externally owned account will be used for the purpose of burning the tokens on each network (Ropsten and Mainnet). The account will be used for executing the events on Ropsten as well as on Mainnet. The accounts will be used for this purpose only. Their private keys will be destroyed afterwards. The tokens to be burned will remain under the sole control of DigitalBits during the burning process. Quantstamp will not have access to the private keys for the accounts. All the actions outlined below will be carried out by the DigitalBits. The sequence of actions will be carried out first on Ropsten and then on Mainnet.

Ropsten

1. All tokens to be burned will be collected under account 0x24800aB372B37169507c82B1e839b783E336246c by the DigitalBits team, along with an estimated of no less than 0.2 Ether for covering gas fees. The balance will be verified and recorded in this report before proceeding to the next steps. The expected balance is 985,000,000,000,000,000 (which includes the 7 decimal places of the token).
2. For the convenience of the DigitalBits team, the transaction will be issued through the verified source code of the token contract on Etherscan with Metamask as a web3 provider and offline transactions signing by Ledger hardware wallet.
3. The DigitalBits team will call method burn() with value 100,000,000,000 (that is 10,000 XDB with 7 decimals) and wait for the transaction to be mined. It is expected that the total supply, returned by method totalSupply(), will decrease to 99,999,990,000 XDB (999,999,900,000,000,000 including decimals) and the balance of 0x24800aB372B37169507c82B1e839b783E336246c, as returned by method balanceOf(), will decrease by 10,000 XDB down to 98,499,990,000 XDB (984,999,900,000,000,000 including decimals).
4. The balances will be verified and recorded in this report.
5. The DigitalBits team will call method burn() with value 984,999,900,000,000,000 (that is, 98,499,990,000 XDB with 7 decimals) and wait for the transaction to be mined. It is expected that the total supply, as returned by method totalSupply(), will decrease to 1,500,000,000 XDB (15,000,000,000,000,000 including 7 decimals) and the balance of 0x24800aB372B37169507c82B1e839b783E336246c, as returned by method balanceOf(), will decrease by 98,499,990,000 XDB down to 0.
6. The balances will be verified and recorded in this report.
7. The balances will be verified and recorded in this report after at least 20 additional blocks have been mined. If still present, the actions performed will be considered persisted in blockchain and final.

Mainnet

The tokens will be burned in 9 batches. Therefore, the steps 8 through 11 will be repeated 9 times. The final step 12, which will confirm the success of the entire process, will be performed only once after the burning concludes.

8. All tokens to be burned will be collected under account 0x24800aB372B37169507c82B1e839b783E336246c by the DigitalBits team, along with an estimated 0.2 Ether for covering gas fees. The balance in each batch of burning will be verified and recorded in this report before proceeding to the next steps. The expected balances in the individual batches are:
    i. 100,000,000,000 (which includes the 7 decimal places of the token);
    ii. 25,000,000,000,000,000 (which includes the 7 decimal places of the token);
    iii. 29,997,189,310,100,000 (which includes the 7 decimal places of the token);
    iv. 25,194,741,340,000,100 (which includes the 7 decimal places of the token);
    v. 49,807,969,349,900,000 (which includes the 7 decimal places of the token);
    vi. 50,000,000,000,000,000 (which includes the 7 decimal places of the token);
    vii. 125,000,000,000,000,000 (which includes the 7 decimal places of the token);
    viii. 280,000,000,000,000,000 (which includes the 7 decimal places of the token);
    ix. 399,999,999,999,999,900 (which includes the 7 decimal places of the token).
9. For the convenience of the DigitalBits team, the transaction will be issued through the verified source code of the token contract on Etherscan with Metamask as a web3 provider and offline transactions signing by Ledger hardware wallet.
10. The DigitalBits team will call method burn() with the total balance of the account (as listed in step 8) and wait for the transaction to be mined. It is expected that the total supply will decrease gradually decrease to 1,500,000,000 XDB and after each batch will be:
    i. 999,999,900,000,000,000 (which includes the 7 decimal places of the token);
    ii. 974,999,900,000,000,000 (which includes the 7 decimal places of the token);
    iii. 945,002,710,689,900,000 (which includes the 7 decimal places of the token);
    iv. 919,807,969,349,899,900 (which includes the 7 decimal places of the token);
    v. 869,999,999,999,999,900 (which includes the 7 decimal places of the token);
    vi. 819,999,999,999,999,900 (which includes the 7 decimal places of the token);
    vii. 694,999,999,999,999,900 (which includes the 7 decimal places of the token);
    viii. 414,999,999,999,999,900 (which includes the 7 decimal places of the token);
    ix. 150,000,000,000,000,000 (which includes the 7 decimal places of the token).

    The balance of 0x24800aB372B37169507c82B1e839b783E336246c will decrease down to 0 after each burn.

11. The balances after each batch of burning will be verified and recorded in this report.

12. The balances will be verified and recorded in this report after at least 20 additional blocks have been mined. If still present, the actions performed will be considered persisted in blockchain and final.

Possible complications

The following complications may occur during the process:

1. **The original balance may be collected under a wrong account by mistake or by an adversary.** This is a critical irreversible step for which the DigitalBits should take responsibility. If tokens are collected under an account under nobody's control, they can be considered effectively burned. If there is a risk that the tokens get collected under an adversary account, token migration will be necessary.
2. **The Ledger hardware wallet is not initialized with the proper private key.** The mnemonic used to generate the private key must be safely recorded by DigitalBits. The key will be recovered, the Ledger will be reinitialized with it, and the process will continue.
3. **The projected transactions are not be permanently persisted due to an uncled chain fork.** This would be observed during the process or after waiting for the final confirmation, and will exhibit itself by a discrepancy in balances or failing transactions. The uncled transactions for steps will need to be issued again.

3. Execution

The action described in Section 2 were executed and can be witnessed in the following blocks:

Ropsten

Burn of Tokens

1. Completed and verified in block #6864749. The balance is 98,500,000,000 XDB (985,000,000,000,000,000 including 7 decimals).
2. Completed.
3. Completed November 28, 2019, 9:26am EST and mined in block #6865043. The transaction hash is: 0xe00f10f843e726c0ec1b77fa84b508d49ec7d8d85914bb36aca820d008e06391

4. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 98,499,990,000 XDB (984,999,900,000,000,000 including 7 decimals) and total supply of XDB is 999,999,900,000,000,000 (including 7 decimals) in block #6865043.
5. Completed on November 28, 2019, 9:31am EST and mined in block #6865059. The transaction hash is: 0xab6db1bd1bce5a16faf263bd1f07430337b9891b306f68e4365e2cecc3b2bb86
6. The balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and the total supply of XDB is 1,500,000,000 XDB (15,000,000,000,000,000 including 7 decimals) in block #6865059.

Final confirmation

7. The balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and the total supply of XDB is 1,500,000,000 XDB (15,000,000,000,000,000 including 7 decimals) in block #6866249.

Mainnet

Batch 1

8. Completed and verified in block #9015969. The balance is 10,000 XDB (100,000,000,000 including 7 decimals). The total supply of XDB is 100,000,000,000 XDB (100,000,000,000,000,000 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 9:34am EST, and mined in block #9015975. The transaction hash is: 0x7b81b256e15817c8be2f1006c7d47d831f793f2db9ccc922c865c75b7369d255.
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 999,999,900,000,000,000 in block #9015975.

Batch 2

8. Completed and verified in block #9016008. The balance is 2,500,000,000 XDB (25,000,000,000,000,000 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 9:42am EST, and mined in block #9016017. The transaction hash is: 0x6e217f5265f6cd0ce23778d3e2c7554ef64835f9f523efe43910732fcc84eb01 .
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 974,999,900,000,000,000 in block #9016022.

Batch 3

8. Completed and verified in block #9016032. The balance is 2,999,718,931.01 XDB (29,997,189,310,100,000 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 9:51am EST and mined in block #9016043. The transaction hash is: 0x5a1b7dcf9b77cf3b04bb1d14f09706736063fa029fdeb8f65ef65106ca79a3cd.
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 945,002,710,689,900,000 in block #9016044.

Batch 4

8. Completed and verified in block #9016061. The balance is 2,519,474,134.00001 XDB (25,194,741,340,000,100 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 9:57am EST, and mined in block #9016068. The transaction hash is: 0x3d51337ddfb720ae2a26293ccc65556bec3b675f5949204281f7bd7813fc2076.
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 919,807,969,349,899,900 in block #9016073.

Batch 5

8. Completed and verified in block #9016082. The balance is 4,980,796,934.99 XDB (49,807,969,349,900,000 including 7 decimas).
9. Completed.
10. Completed on November 28, 2019, 10:02am EST, and mined in block #9016090. Transaction hash is: 0x64477b28090551d8272221eba5293e1aec62e712e3fb07eb4655edad9e8f282e.
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 869,999,999,999,999,900 in block #9016091.

Batch 6

8. Completed and verified in block #9016104. The balance is 5,000,000,000 XDB (50,000,000,000,000,000 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 10:09am EST, and mined in block #9016108. Transaction hash is: 0x65010c22e775f80abceabd87fb13eec21e09cd0bbf95c105ba3a877c3d32405a.
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 819,999,999,999,999,900 in block #9016112.

Batch 7

8. Completed and verified in block #9016123. The balance is 12,500,000,000 XDB (125,000,000,000,000,000 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 10:15am EST and mined in block #9016131. Transaction hash is 0xf5b3eb584371e8b3947a5b243fd8644d743365599f75c208fec5bd38c7a0d20f.
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 694,999,999,999,999,900 in block #9016132.

Batch 8

8. Completed and verified in block #9017369. The balance is 28,000,000,000 XDB (280,000,000,000,000,000 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 3:38pm EST and mined in block #9017376. Transaction hash is 0xbfbd2a61ce224efb30adfc95093c7429abf5fc5ebb67b21be83adc00d8a6e560 .
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 414,999,999,999,999,900 in block #9017376.

Batch 9

8. Completed and verified in block #9017399. The balance is 39,999,999,999.99999 XDB (399,999,999,999,999,900 including 7 decimals).
9. Completed.
10. Completed on November 28, 2019, 3:45pm EST and mined in block #9017407. Transaction hash is 0xbacc5333e4a1ce8a7cee385e72bc36fa5be7b2b0790c0a87db07d455e818cd38 .
11. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 150,000,000,000,000,000 in block #9017407.

Final confirmation

12. Balance of 0x24800aB372B37169507c82B1e839b783E336246c is 0 and total supply of XDB is 1,500,000,000 (150,000,000,000,000,000 including 7 decimals) in block #9017528.

4. Significant Block References

Ropsten

Block Before Burn	
Height	6864749
Hash	0xf0773ef343d488c3518d549a0642670b03480108b3c72a92c1e0e330a1ada0de
Parent hash	0x9bdb60c40954725db95d500947a5c6c0b621823dceeaac3a36f68c311851c02e
Timestamp	Nov-28-2019 01:19:59 PM +UTC
Total supply of XDB	100,000,000,000.0000000 XDB
Balance of 0x24800aB372B37169507c82B1e839b783E336246c	98,500,000,000.0000000 XDB

Confirmation Block	
Height	6866249
Hash	0xa5d74dc1ec704648f9d544a937afc7c77d8620e7f6f2eb4b499315161c642a3e
Parent hash	0x3d18ecf21343191cdca6ec796ef6eb86b6930885ae94433035ba9b64da49ca8d
Timestamp	Nov-28-2019 07:08:12 PM +UTC
Total supply of XDB	1,500,000,000.0000000 XDB
Balance of 0x24800aB372B37169507c82B1e839b783E336246c	0 XDB

Mainnet

Block Before Burn	
Height	9004707
Hash	0x76ca3ab7701650727b45e8efd8ce4083ff72ebf9319fa6463a8054d7a894adb8
Parent hash	0x280bf7221932397737846b1578b79404ed83c0f2437dd47ff971b0325f7e47ad
Timestamp	Nov-26-2019 02:39:08 PM +UTC
Total supply of XDB	100,000,000,000.0000000 XDB
Balance of 0x24800aB372B37169507c82B1e839b783E336246c	0 XDB

Confirmation Block	
Height	9017528
Hash	0xdae318a84922d73d8ecf39880e501a6c53a7abd8df8a76d386e93000fcdbf542
Parent hash	0xc78f2a753f1ca39cbde1004297265e0b43ea1a93faa4d21d88f9c8cb4270158f
Timestamp	Nov-28-2019 09:15:19 PM +UTC
Total supply of XDB	1,500,000,000.0000000 XDB
Balance of 0x24800aB372B37169507c82B1e839b783E336246c	0 XDB