CSE 598 Project 2 Part 1 Report

Title: Creating a financial transaction on Dash public blockchain

Student Name: Harshith Chittajallu

ASU ID: 1218707243

Abstract:

In this project, we used a Dash library in NodeJS programming language for writing transactions on the Dash blockchain network (the testnet). The given codebase file contained the address of the sender and authentication token. We get the amount available with the sender by accessing the URL in the main JavaScript file. If the amount available with the sender is greater than or equal to the send amount given in the main file, then we create a transaction using dash core library and send the transaction using chainRider. This nets us the transaction ID, indicating that our transaction is successful.

Keywords:

Dash, Token, Transaction ID, chainRider, NodeJS, JavaScript, address

Introduction:

Bitcoin is the most popular public blockchain out there for sending payments. However, while Bitcoin might be the oldest option, it is most certainly not the best because of its transaction confirmation time.

Dash, on the other hand thrives in fast transaction confirmation and is our choice for this project because of its applicability in a broad range of industrial use-cases concerning fast digital payments. Transactions enable users to send and receive payments on the Dash blockchain. The cryptocurrency is also named Dash which is a collection of duffs [6]. Each transaction is constructed out of several parts which enable both simple direct payments and complex transactions. A transaction has at least one input and one output. Each input spends the dash amount paid to previous output and each output then wait an Unspent Transaction Output (UTXO) until a later input spends it.

An input uses a transaction identifier (TXID) and an output index number (often called "vout" for output vector) to identify a particular output to be spent. It also has a signature script which allows it to provide data parameters that satisfy the conditionals in the pubkey script. In this report, we obtain the TXID after successfully creating a transaction between a sender and a receiver.

Terminology:

Dash:

Dash is an open source blockchain and cryptocurrency focused on offering a fast, cheap global payments network that is decentralized in nature. According to the project's white paper, Dash seeks to improve upon Bitcoin (BTC) by providing stronger privacy and faster transactions. [2]

Bitcoin:

Bitcoin is both a form of currency and a technology that uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. [1]

UTXO:

The term UTXO refers to the amount of digital currency someone has left remaining after executing a cryptocurrency transaction such as bitcoin. [3]

Duffs:

Denominations of Dash value usually measured in fractions of a dash but sometimes measured in multiples of a duff. One dash equals 100,000,000 duffs. [4]

TXID:

An identifier used to uniquely identify a particular transaction; specifically, the sha256d hash of the transaction. [5]

Goal Description: Our main goal in this project is to complete the given code base and create a transaction in Dash. When successful, we need to obtain the transaction ID as a proof of the result.

Steps to followed:

1. Write a function that sends {send_amount} of dash from {sender} to {receiver} in the given codebase
2. [second goal written as at least one complete sentence] Register on ChainRider to get a ChainRider token (instructions provided) and input its value as {token}
3. Verify which of the following addresses has money use that address as sender and the other address as receiver
4. Create a transaction using the {dashcore} library, and send the transaction using ChainRider
5. Send Raw Transaction API
6. Execute the code in NodeJS using terminal
7. Obtain the resulting transaction ID

Description of proposed solution:

I created 2 function statements as per our goals. There were also certain preliminary steps which I had to figure out to execute the code properly.

Procedure followed:

1) Preliminary step1: Installed Dash library in NodeJS

2) Preliminary step2: Installed got library in NodeJS

3) Preliminary step3: Obtained the URL to send the amount

4) In the code base, created a variable which uses the got function to receive the amount left with the sender and stored it.

5) Created an error function to go along with the above function for debugging

6) Created the main function. This has a for loop to detect the amount left in the sender's wallet. Then used a conditional statement to send a certain amount to the receiver if the sender has that amount.

7) Generated the transaction details including the raw id and the token value and stored them in a temporary object.

8) Used the URL to send the amount to the server and get the hashed value.

9) Running the code gave successfully gave the transaction ID.

Issues Faced and Methods used to resolve them:

Some of the issues faced while execution were as follows:
"Error: Cannot find module 'dash'"
"Error: Cannot find module 'got'"
Most likely the errors above were caused by a failed download of the dash and got libraries. Reinstalling them fixed this issue.

"TXID: ' ' "

Code did not have any errors, but the transaction ID was being displayed as null. This was a syntax error on two fronts, one where the stored variable was not being displayed and the other being the display code itself. Changed these after referring debugging using online references.

Related Works:

https://www.chainrider.io/docs/dash/#send-raw-transaction

https://dashplatform.readme.io/docs/introduction-what-is-dash

Result & Conclusions:

Obtained transaction id:
0558c04b1a8073e236526f64cdba7731daebbc1b23a49f615413419a42a7f50d

From this project, I have learnt how to create a successful transaction in Dash using NodeJS. This required learning to understand the NodeJS software as well as the Dash framework. Now that I know the intricacies that go into coding a transaction in cryptocurrencies, I will be able to develop better frameworks or even look into mining as a possible financial revenue stream. This project has been an extremely important steppingstone into the world of the cryptocurrency, and I am quite glad that I can take part in learning more about this secure technology.

Bibliography:

[1] https://bitcoin.org/en/

[2] https://coinmarketcap.com/currencies/dash/

[3]
https://www.investopedia.com/terms/u/utxo.asp#:~:text=What%20Is%20UTXO%3F,used%20to%20balance%20the%20ledger.

[4] https://dashcore.readme.io/docs/core-ref-transactions

[5] https://dashcore.readme.io/docs/core-guide-transactions

[6] https://canvas.asu.edu/courses/70154/files/24552971/download?download_frd=1