TECHNICAL WHITEPAPER

DIM Ecosystem

HYBSE / DEPOTWALLET/ DIMCOIN / DIM CURRENCIES / NEM

Based on NEM Technology

Author:

DIMCOIN FOUNDATION

Version: V.0.4 - Date: 21.06.2017

Abstract

The equity market has a very inefficient system when it comes to transfers and settlements. In a conventional system, traders are limited when making payments to trade stocks, and somewhat restricted in transfers. We think the system should be revamped to make trading more efficient and easier for traders. To achieve this, we have considered blockchain technology, which is extremely secure and robust, despite it being decentralized. This paper only touches the surface of the concept and principles of our system and it is targeted towards a wide range of readers. It is kept as simple as possible to give a basic technical idea of how DEPOTWALLET works in conjunction with HYBSE, how DIMCOIN and DIM Currencies work synergistically, hand in hand, in order to create an Ecosystem that will revolutionize how equity markets work.

Table of Contents

03 Blockchain Technology
04 DIM Ecosystem based on NEM Technology
05 NEM Technology/Namespaces and Mosaics
06 Definition of Namespaces and Mosaics
07 How trading works
08 What is DIMCOIN
08 Detailed Specification of DEPOTWALLET
10 How DEPOTWALLET works
11 Buying HYBSE Assets with DIM Currency
12 HYBSE Price API
13 Showing value of HYBSE Assets
14 HYBSE Matching Diagrams
16 References, Links and Sources

Blockchain Technology

Blockchain technology is a decentralised ledger solution with **enhanced security and it is suitable for financial transactions.** Many of them are simple solutions while a few are fully featured, powerful, simple in design, and most importantly, **inexpensive to operate.**

Blockchain technology does not purport to give a new impetus to existing financial technologies. Rather, it is a very cost-effective solution that will save a tremendous amount of money, time, and labour in comparison with existing technologies. At the same time, blockchain can cut some processes or reduce them to nothing, **there-by possibly saving the industry a lot of running costs.**

The blockchain solution is a technology that is a synthesis of previously well tested and proven technologies. Specifically, the blockchain technology is designed from a combination of:

- Computer peer-to-peer technology
- Cryptography science
- Database system

The end result is a powerful ledger system that is immutable and irreversible, meaning that transactions can not be changed once signed and transferred. Transactions are therefore final and there is no double-spending.

“Blockchain technology is nascent. While the technology itself offers tremendous potential and possibility, the industry is just “waking up” to apply the technology to its financial systems.”

Secure Cryptographic Technology

The use of cryptography science encompasses two factors. The first being the fact that it is used for signing off a transaction by the user; the second being that it is used to proof the transaction so that it cannot be changed. Another feature that is rarely used in blockchain is the encryption of messages.

The DIM Ecosystem based on NEM Blockchain Technology

The DIM Ecosystem (NEM) is a purpose built solution. In addition to the standard undistinguished blockchain solution, it has incorporated special features into its block-chain technology:

- Ability to manage numerous asset transactions. These assets could be assets of different classes such as digital money, securities, precious metals, etc.
- A global namespace solution for unique registration of each set of ledgers within the blockchain ecosystem.
- Simple, out-of-the-box smart contracts in the form of transaction management so that users of the solution can be governed by regulatory requirements.

The DIM Ecosystem based on NEM blockchain technology uses a consensus mechanism to manage every transaction. It consists of a network of nodes (either permissioned or permission-less) networked together in a peer-to-peer (P2P) configuration.

How Transactions Work

Transactions are broadcasted and each P2P node will record these transactions and verify them as they come in. At periodic intervals, called the block time, these transactions are grouped together and the transactions undergo a hash process (digital fingerprinting) linking it to the previous block. They are then added on as a new block of information in the blockchain. The private and permissioned ledger does not have mining per se, and follows a controlled Proof-of-Stake algorithm, while the permission-less (Public Chain) is based on an algorithm called Proof-of-Importance.

Reputation Management / Anti-Fraud Technology

Built into the DIM Ecosystem (NEM) is a mechanism (Eigentrust++ reputation manage-ment algorithm) to ensure each P2P node is reputable and therefore not fraudulent. NEM also created an all-new P2P time synchronisation algorithm to ensure that each node is synchronised with one another in the right time slot.

DIM Ecosystem works with Namespaces and Mosaics of NEM

The most simple way to acknowledge it is the domain and file analogy on the internet. Envision that a domain address has to be unique in a root (minimum level). Namespace addresses this particular feature. If one creates a namespace, that namespace will appear unique in the DIM Ecosystem (NEM). For instance, if one were to create a namespace called “assets” that namespace cannot be created by a second person. Just like on the internet where a domain can have a sub-domain, namespaces can have sub-name-spaces.

Namespaces have two levels of sub-namespace domains giving it a total of up to 3 levels including the namespace. A mosaic is hosted in a file accommodated on a domain and represents an asset. Like a website and directory, a mosaic can have an identical name as other files on other domains. Although a total address of a namespace + mosaic will continually be exclusive as the root namespace is unique even if the rest of it isn‘t.

Mosaics are a very important backbone of the DIM Ecosystem (NEM). Mosaics add depth and breadth into DIM Ecosystem (NEM). Through mosaics, we are now able to do a lot more, opening up a plethora of things that otherwise cannot be done in most blockchain platforms. Coupled with the DIM Ecosystem (NEM) multi-signature, mosaics allow new levels of blockchain utility and versatility.

Examples:

Namespace (root level domain): ASSETS
Sub-domain 1: MARKET
Sub-domain 2: OTC

Mosaics:

STOCKS
TOKENS
ETF

Accordingly, mosaics can be named as such:

ASSETS:STOCKS
ASSETS:TOKENS
ASSETS:ETF
ASSETS.MARKET:STOCKS
ASSETS.MARKET:TOKENS
ASSETS.MARKET:ETF
ASSETS.MARKET.OTC:STOCKS
ASSETS.MARKET.OTC:TOKENS
ASSETS.MARKET.OTC:ETF

Each of the above mosaics is made particular by the namespace’s fully qualified name. The mosaic is also preceded by an “:” to make a distinction from a namespace.
To summarize, everything under the root level domain belongs to the account that created it. In the above examples, the root level domain name is “ASSETS”.

Significance of Namespaces and Mosaics

To understand DIMCOIN and DIM Currencies such as DIM EUR and DIM USD, we will explain NEM Namespaces that give improvements to a unique naming practice while mosaics give rise to the establishment of assets.

The primary release is a mosaic that has the following properties:

Description
Free-text definition of the mosaic up to 128 characters that is changeable by the owner.

Divisibility
Adding this makes a quantity divisible, up to 6 decimal places. A divisibility of 2 means 2 decimal places. DIMCOIN has a divisibility of 6 and DIM Currencies (DIM USD & DIM EUR) have 2.

Information
Arbitrary byte array that can be in the property, with a size limit; this is the same as “messages” in NEM that can be encrypted.

Domain name or namespace (required)
Globally unique fully qualified domain name that is registered and owned by the mosaic creator. A top level namespace has a size limit of 16 characters, sub-namespaces have a limit of 64 characters.

Name (required)
Name of the mosaic, up to a size limit of 32 characters; must be unique under the domain name.

Mutable quantity
The amount of mosaics in circulation. If immutable, it is fixed, otherwise it is dynamic, i.e., more can be created or destroyed later. In case of DIMCOIN we have fixed quantity, and the DIM Currencies (DIM USD & DIM EUR) are dynamic.

Transferability
If no, it means it can only be transferred between user and creator. Otherwise, it is freely transferable between third parties.

Levy
A levy allows the creator of a mosaic to set a tax on any subsequent transactions of that mosaic. This levy is sent to an account of the creator’s choice. Any mosaic or XEM may be used as a levy. In case of DIMCOIN , the DIMCOIN is used as a levy. For Assets we use DIM Currencies (DIM USD & DIM EUR) as levies.

How Stock Trading Works

No broker will be required for trading. Every single investor will trade directly at the stock exchange. The existence of brokers used to needed because it was almost impossible to house all traders and physically trade. Therefore, they were represented by brokers who would hold a seat indvidually on the exchange floor. These seats were replaced by licenses for each member to trade on these stock exchanges when stock exchanges went electronic. Hence, with each of them operating and regulating their own electronic trading platforms for their investors, the licensed members became known as brokers.

Today, it is not necerssary to have an exchange floor because this very same “floor” is virtualised and trades can be done by each and every trader or investor. The computer monitor is a window to the floor and the price bid “shouting” is achieved by keying in the ask and bid prices of any stock by each trader in a trading platform operated by broking firms. To “shout” a price is not needed.

There are also more practical tools that allow traders to make trades directly, **including automated bots and high frequency trading.** That is the past and the present. Nonetheless, to break it up further, the stock exchange could merely do away with licenses for members and alternatively accept direct bidding and asking by investors. The stock exchange will have a repository of money as well as stocks guaranteed by investors to the system in its real-time database. **Trading occurs in real time and it would be able to perform high-frequency trades.**

One immediate advantage of this method is that many stock exchanges can exist, allowing investors to choose which stock exchange they want to trade in. With immediate settlements, exchanges like **HYBSE** and **DEPOTWALLET** can now operate at different times of the day, including having the option to operate 24 hours a day, thanks to **NEM Technology.**

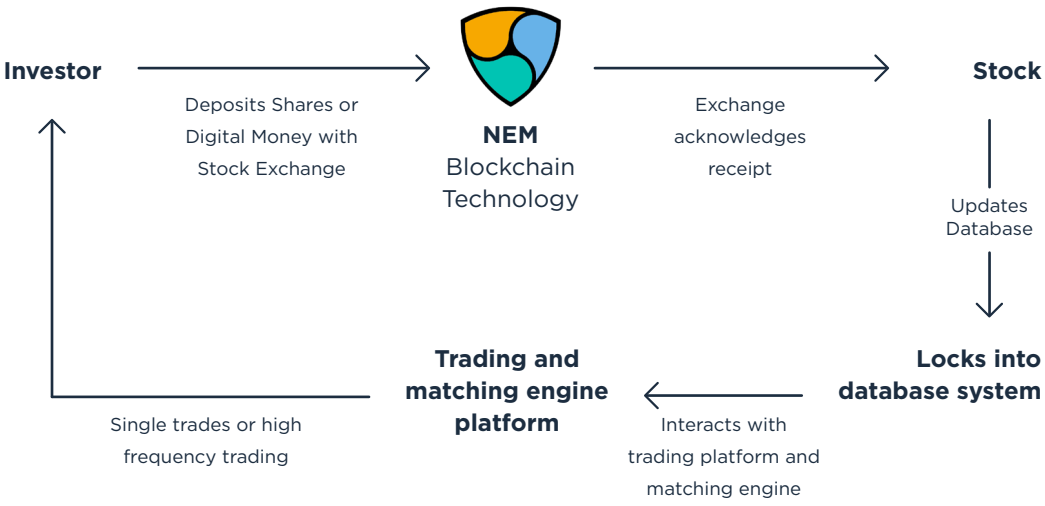

Fig-1: Trading Process

What is DIM?

DIM (Data Interchange Module) is a cryptocurrency based on NEM technology and it is built on blockchain. The NEM blockchain is an improvement on existing blockchain technologies, allowing the DIM to be part of the DIM Ecosystem. The DIM uses elliptic curve cryptography to ensure confidentiality, authenticity and non-repudiability of all transactions.

The DIM cryptocurrency has two versions: DIMCOIN and DIM Currencies.

The DIMCOIN is a speculative coin and it has a quantity commitment of 9 billion coins. The DIMCOIN is tradable on the open market and the DIM Currencies(DIM USD & DIM EUR) are a medium of payment within the DIM Ecosystem. The value of the DIM Currencies is linked to the value of fiat currencies from which they are exchanged. Their supply is determined by the volume of fiat currencies that are exchanged into DIM Currencies.

DEPOTWALLET Specifications

DEPOTWALLET is built on the NEM Nanowallet. The software is powered by AngularJS 4.0, ExpressJS and few NodeJS modules. For UI, it is powered by Bootstrap 4 and jQuery (single plugin). Gulp has been used as the package manager and compiler for typescripts and Sass.

The software communicates with various NEM Supernodes/nodes, currency exchange servers and HYBSE servers through API to get users‘ account data, other blockchain information and currency exchange data for XEM, Bitcoin, USD, EUR and HYBSE stock prices.

Accounts have private and public Ed25519 key pairs, and they are associated with a mutable state that is updated when transactions are accepted by the network. Accounts are identified by DEPOTWALLET addresses, which are derived in part from one way mutations of Ed25519 public keys.

Transaction on the DIM Ecosystem (NEM Technology)

Transactions introduce dynamism into a DIM Ecosystem. They are the only way of altering the state of an account. A newly created transaction that has not yet been included in a block is called an unconfirmed transaction. Unconfirmed transactions are not guaranteed to be included in any block. As a result, unconfirmed transactions have no effect on the account state. The account state is only updated when a transaction is included in a harvested block and thereby confirmed.

Fees on DEPOTWALLET/Stamps (XEM)

Different types of transactions exist. Each type has a specific purpose, e.g. transfer DIMCOIN from one account to another or convert an account to a multisig account. Since transactions consume resources of the NEM P2P network, there is a fee STAMP (XEM) for each transaction. The fee depends on the transaction type and other parameters of the transaction. Transactions have a deadline and if a transaction is not included in a block before its deadline, the transaction is considered expired and gets dropped by the network nodes.

The key features of DEPOTWALLET include:

- Simple and asset transfers (Mosaics on NEM Technology)
- Create and edit multi-signature contracts (Future feature)
- Plain & encrypted messaging
- Transactions to alias (@namespace)
- BIP32 accounts
- NCC wallet support
- Balance to BTC and USD
- Simple transaction using QR code

How DEPOTWALLET Works

DEPOTWALLET works as a digital wallet for the crypto assets. In DEPOTWALLET, users may perform four actions: buy DIMCOIN and HYBSE assets, sell DIMCOIN and HYBSE assets. Besides those buy/sell processes, users can transfer those assets (a.k.a. mosaics) to other DEPOTWALLET users.

Buying DIMCOIN:

To buy DIMCOIN, users should use the following method:

- Browse to the DIMCOIN page on DEPOTWALLET, where all the DIMCOIN packages are listed,
- Select the desired DIMCOIN package,
- Upon selecting the DIMCOIN package, users are taken to the transfer page where the transfer form is populated with pre-filled data. The data contains users‘ addresses as the senders, admin addresses as the recipient and DIMCOIN package details,
- Users enter their passwords and submit the form,
- The message is received by admin,
- Users are requested to deposit the money,
- DIMCOIN are transferred to users’ accounts once the money is received

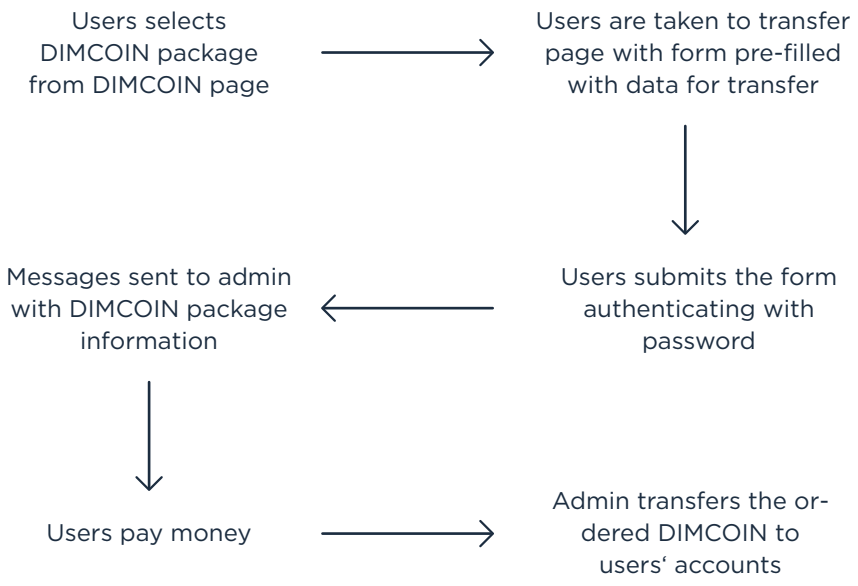

Fig-2: DIMCOIN buy processes

Buying HYBSE Assets

To buy HYBSE assets, users follow these methods:

- Users browse to the assets explorer page on DEPOTWALLET, where all the available HYBSE assets are listed with their current prices. The prices for HYBSE assets are fetched from HYBSE API for the associated stocks,
- On the list, users enter the amount of HYBSE assets they want to buy. The users are limited to buy HYBSE assets with the available DIM Currencies in their accounts.
- Upon clicking the buy button, users are taken to the transfer page where the transfer form is populated with pre-filled data. The data contains the users' addresses as senders, admin addresses as recipient, HYBSE asset details, transfer fees and encryption fees. The DIMCOIN mosaic is also attached with the calculated amount (the price of HYBSE assets in DIM Currencies multiplied by the amount of assets),
- Users enter their passwords and submit the forms,
- The transfers are initiated,
- Upon transfer confirmation, HYBSE assets that are bought are transferred to the users' accounts,
- On HYBSE, the same quantity of stocks are transferred to users' accounts. The users in HYBSE are identified by their DEPOTWALLET addresses.

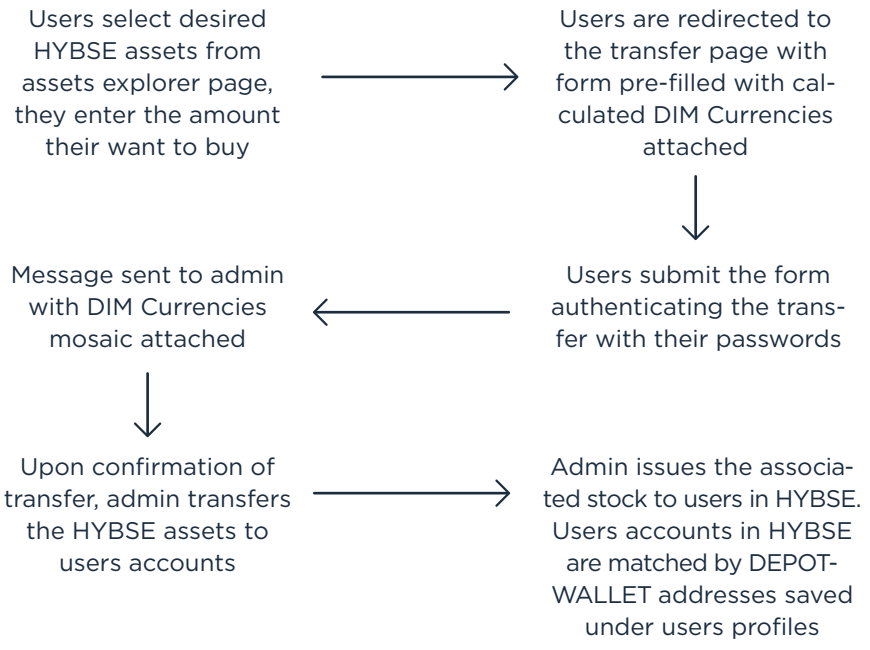

Fig-3: HYBSE assets buy processes

HYBSE PRICE API - Showing USD/EUR prices of owned DIMCOIN

To show the USD/EUR value of DIMCOIN owned by the users, the following processes are performed by the application:

- Exchange rate data requested to cryptocurrency API
- DIM to BTC rate is taken from API data
- Exchange rate data requested to forex API
- BTC to USD/EUR rate is taken from API data
- On widget USD/EUR rate is shown following the calculation (DIM_BTC rate * BTC_EUR rate) and a total value of user owned DIMCOIN is shown (User owned DIMCOIN * DIM_BTC rate * BTC_EUR rate)

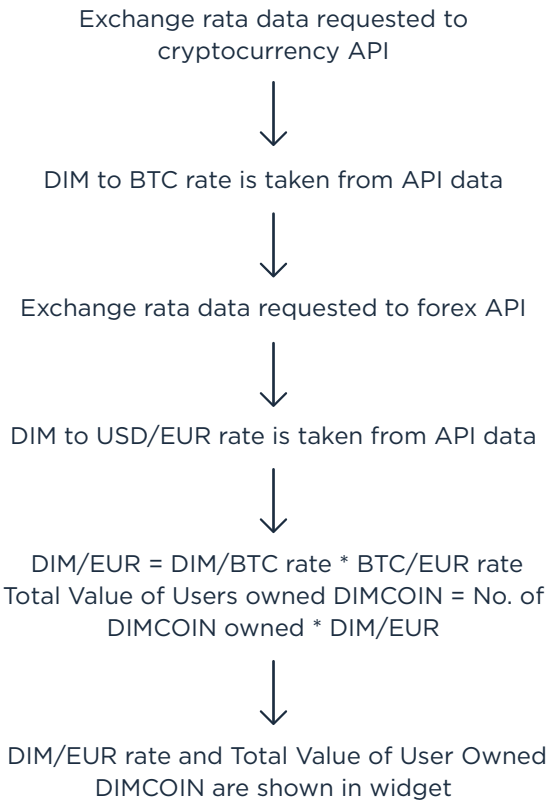

Fig-4: How USD/EUR exchange value shown for DIMCOIN

Showing the value of owned HYBSE assets

To show the value of HYBSE assets owned by users, the following processes are performed by the application:

- Rate requested to HYBSE API providing the names of the assets (mosaic on NEM Technology)
- HYBSE API matches the mosaic names with associated company registered in HYBSE
- Latest stock prices fetched for the stock based on the Stock ID (HBOTC-X)
- API response sent with retrieved data
- On the widgets, HYBSE asset rates are shown and the total value of user-owned HYBSE assets are shown (User-owned HYBSE assets * stock prices received using HYBSE API)

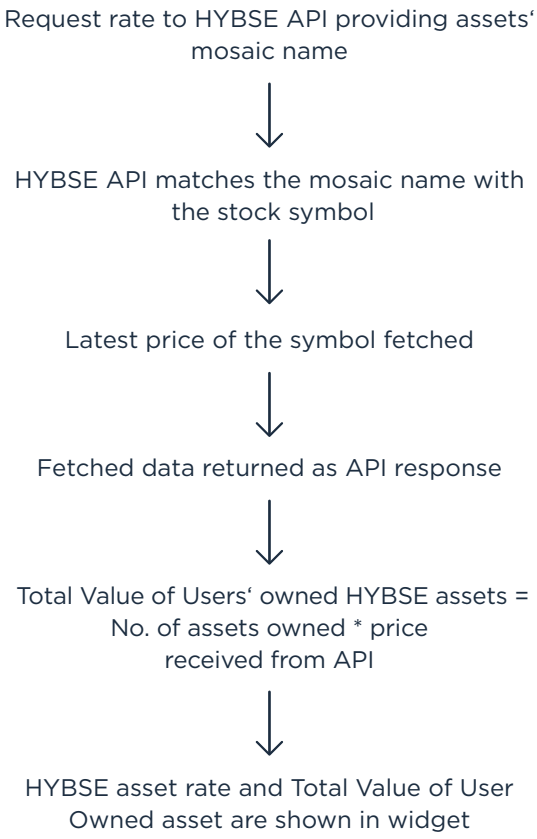

Fig-5: How value of HYBSE Assets shown

HYBSE Order Matching Diagrams

Buy Order Matching

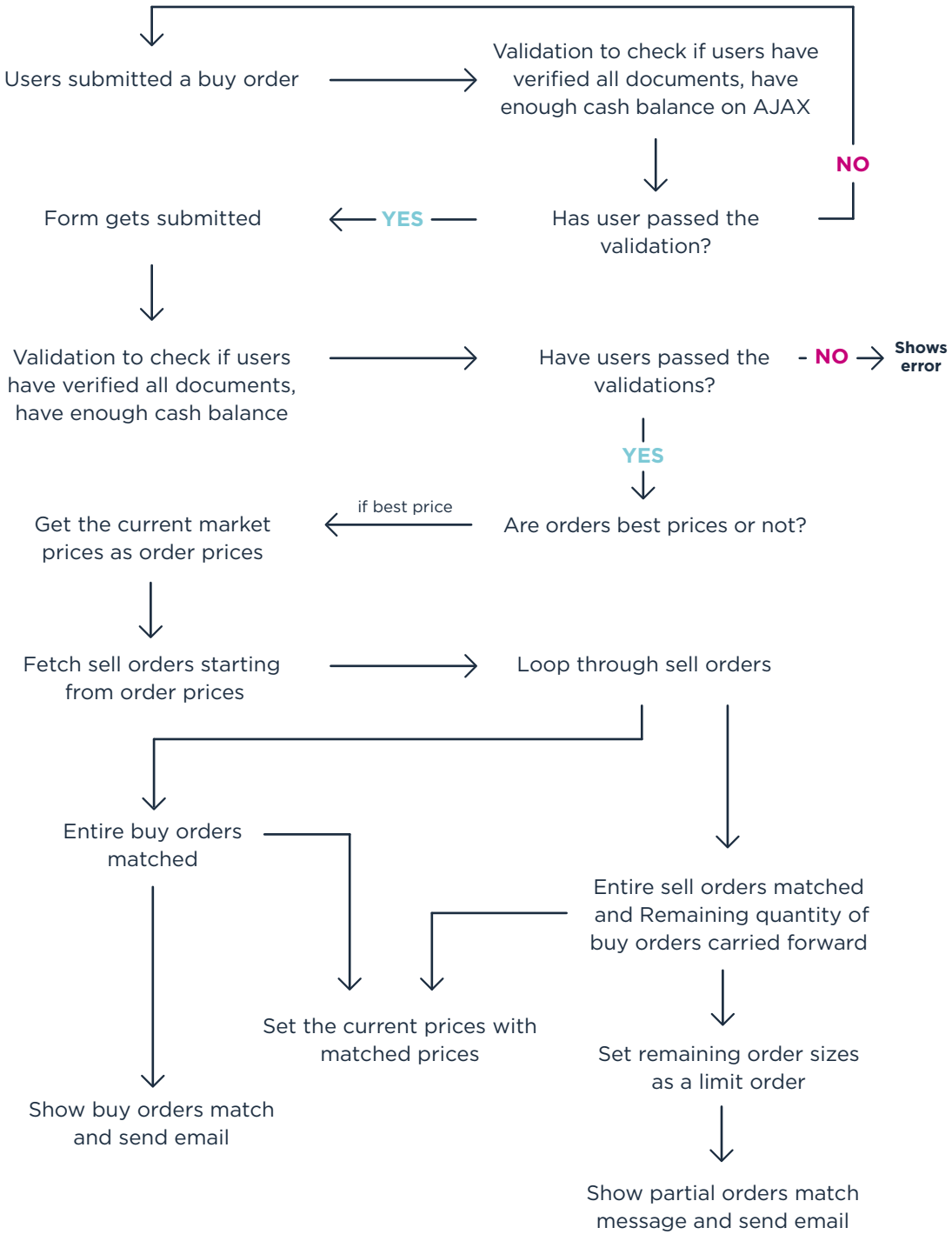

Fig-6: HYBSE Buy order match processes

Sell Order Matching

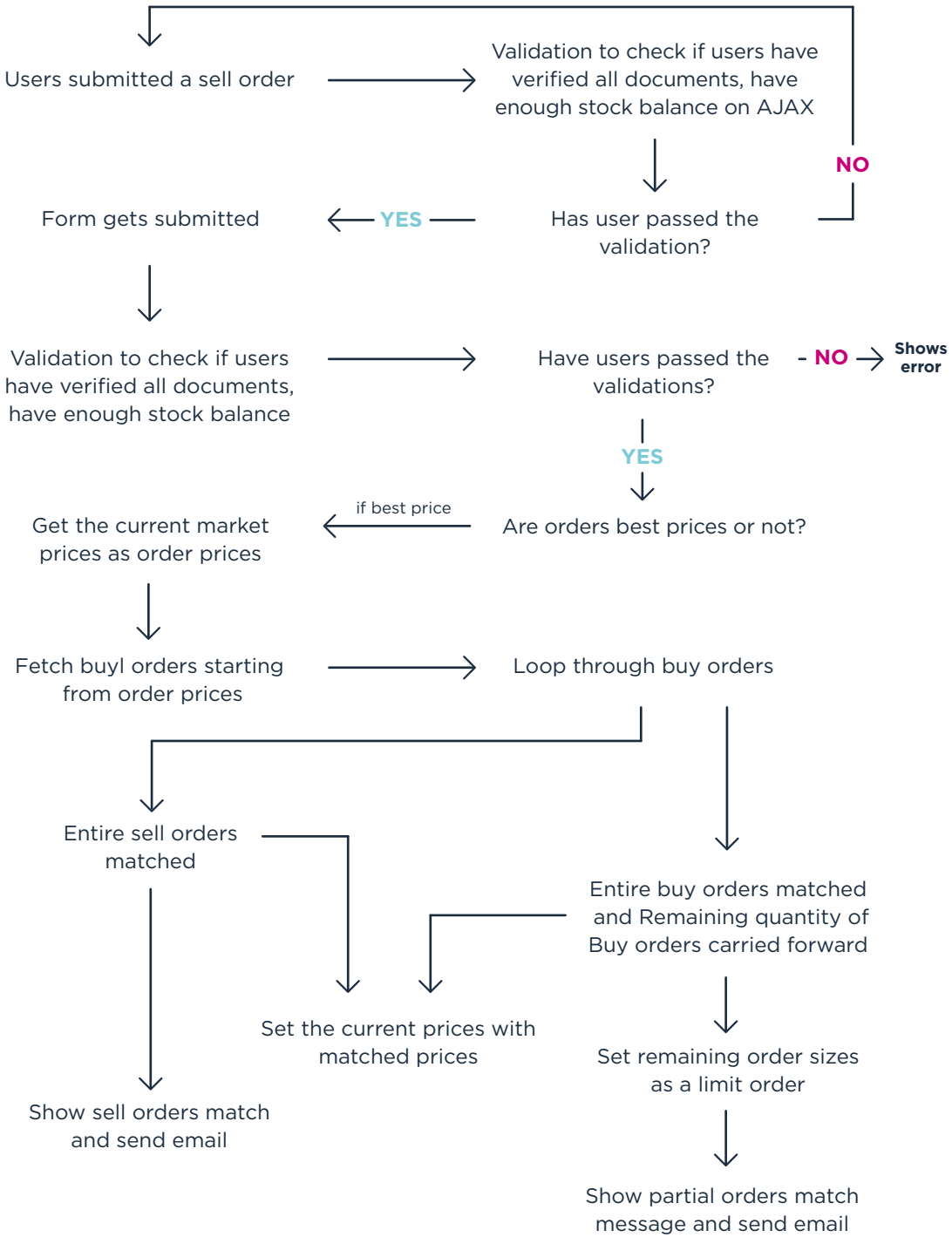

Fig-7: HYBSE Sell order match processes

Websites / References

Online Stock Market
https://hybse.com

DEPOTWALLET Online Wallet
https://DEPOTWALLET.com

DIM Ecosystem
ICO Website
https://dimcoin.io

Sources / Links:

Nem Technical Reference
https://www.nem.io/NEM_techRef.pdf
Version 1.0 - May 15, 2015

Radicalizing the Equity Market Landscape through NEM Blockchain Technology
https://nem.io/RadicalizingEquityMarket.pdf
LON WONG - April , 2017