Switcheo Network: Multi Chain Decentralized Exchange

Ivan Poon <ivan.poon@switcheo.network>
Henry Chua <henry.chua@switcheo.network>
Jack Yeu <jack.yeu@switcheo.network>
Sng Ping Chiang <pingchiang.sng@switcheo.network>

https://switcheo.network
http://switcheo.exchange

2 February 2018
v1.0

CRYP2NOVA

Abstract: *Switcheo is a Decentralized Exchange to be built on top of multiple popular blockchains to facilitate the exchange of digital assets. It will first be launched on the NEO blockchain and will include digital assets such as NEP-5 tokens (e.g. RPX, QLC) and future NEP-X tokens, and NEO's system assets such as NEO and GAS. Trade settlements are done peer-to-peer via interaction with our smart contract(s). Switcheo aims to achieve a network of DEX with cross-chain swapping capabilities between multiple popular blockchains such as QTUM (QRC20) and Ethereum (ERC20), with more research being done for upcoming blockchains like Stellar.*

Archived copy · cryp2nova.com

IMPORTANT NOTICE

This document (the "Whitepaper") has been prepared by Switcheo Exchange Pte. Ltd. ("Switcheo"), and this notice is intended for all readers who view or access it, regardless of the communication channel or platform. The Whitepaper is strictly for information purposes only, and shall not, under any circumstances, be treated as an offer of securities or an invitation to participate in any regulated investment scheme, howsoever defined in any jurisdiction around the world. In addition, none of the information contained herein is intended to form the basis of any advice or inducement to engage in any sort of investment activity.

You are strongly encouraged to read the entire Whitepaper and familiarise yourself with all the information set out below, particularly in the section entitled "Risks and Disclaimers". Please seek independent advice from your professional advisors, including lawyers, tax accountants and financial advisors, if you have any issues, uncertainties or doubts as to any of the matters presented in the Whitepaper.

1. PREFACE

We saw the opportunity to develop a decentralized exchange ("DEX") with the increasing popularity of projects built on the NEO blockchain, and the difficulty of listing such NEP-5 tokens on credible exchanges. We want to reduce the dependency on centralized exchanges for the listing of NEP-5 tokens. Switcheo participated in the first City of Zion's NEO dApp challenge and clinched the 1350 GAS prize. [1] Switcheo aims to be the first DEX launched on the NEO platform, and our future roadmap includes working on cross-chain swaps for QRC20 tokens on the QTUM blockchain and ERC20 tokens on the Ethereum blockchain.

2. INTRODUCTION

With the increasing popularity of blockchain technologies fuelling the price of cryptocurrencies, a majority of these trades are done via traditional centralized exchanges. Centralized exchanges fall into two categories: those that accept fiat currencies (government-backed currencies), and those that do not. Switcheo will initially not accept fiat currency transfers and will first work towards a **multi chain decentralized cryptocurrency exchange** platform where users may perform trades of virtual tokens and assets trustlessly (i.e. without the need to trust a centralized third party).

3. PROBLEMS WITH CENTRALIZED EXCHANGES

3.1 SECURITY

An immediate disadvantage when using a centralized exchange is the security risks arising from the centralization of funds. As all funds sent in by users for trading are stored and secured by the exchange, the funds are prone to a single point of failure. For example, the exchange servers could be breached by attackers, or the exchange's wallet private keys could be lost, resulting in a loss of funds.

Archived copy · cryp2nova.com

These failures are completely out of the control of the individual user, regardless of how secure their passwords are, and they have to trust that the centralized exchange have done what is necessary to secure their funds. There have been major breaches of users' trust, evidenced in past exchange hacks which have amounted to billions of dollars in value lost over the last few years. A prime example of this would be the USD 500 million lost in the recent Coincheck breach. [2]

Decentralized exchanges solve this problem by letting the blockchain and the user handle the security of funds from start to end. A DEX is therefore as secure as its smart contract, and most existing DEXs have been running for a long time with no core breaches (e.g. EtherDelta).

3.2 CONTROL OF FUNDS

When users deposit their funds into a centralized exchange, their funds are under the control of the exchange. The exchange may be able to withhold funds from users[3] or remove funds from users' accounts[4] at any time. In general, a user has to trust that a centralized exchange will always act in good faith for the user. This is in contrast to cryptocurrency's spirit of decentralization and trustlessness.

3.3 EASE OF TRANSFER

Users may also be unable to withdraw assets in small numbers from centralized exchanges[5], or it may not be viable to withdraw often due to high withdrawal fees. This hurts the user's security even further as they are at the mercy of the centralized exchange while their funds remain there. Furthermore, a high number of confirmations are typically required when depositing funds. These issues make trading on centralized exchange a hassle — moving funds from a wallet to an exchange to trade and then back is generally slow and tedious and subject to unanticipated delays.

As all exchange interactions for Switcheo are done via a smart contract (i.e. code on the blockchain), users can buy or sell tokens directly from their wallet, without additional transfers. Users can also withdraw any amount of tokens from their balance at any time, and this is guaranteed by the code of the smart contract. When not actively trading, users' funds are always secured by the same mechanism - their own wallet contract, or Switcheo's smart contract.

3.4 IMMEDIATE LISTING

A big issue with the acquisition of tokens of an early stage blockchain startup is finding exchanges that list the wanted tokens. On the other hand, users who have purchased tokens during an Initial Coin Offering (ICO) also have to wait for the token to be listed on an exchange before being able to sell it. This leaves many users stuck with the token even though they may no longer want it.

With the increasing popularity of projects developed on the NEO Blockchain, Switcheo will strategically start trading NEP-5 Token contracts for the NEO Blockchain first, before moving on to QRC20 Tokens (QTUM). Using the dynamic call functionality of the NEO blockchain, users will be able to list and buy tokens the moment they are available for transfer on the blockchain.

3.5 EXCHANGE FEES

CRYP2NOVA

Archived copy · cryp2nova.com

While centralized exchanges like Binance and Gate.io charge exorbitant rates for withdrawals for small amounts of cryptocurrencies, there will be no withdrawal fee for Switcheo's smart contract. Users will only pay the standard network fees, and not be charged additional amounts should they decide to withdraw their balance. The maker and taker fee for Switcheo is capped at 0.5%, and is guaranteed by the smart contract.

4. PROBLEMS WITH EXISTING DECENTRALIZED EXCHANGES

While a DEX has clear advantages over a centralised exchange in the security & control of funds, ease of transfer, immediate token listing, and lower fees, Switcheo's true priority is to overcome the shortfalls of existing DEXs.

4.1 USER EXPERIENCE

Order mistakes, wrong trades and mis-clicks are the hallmarks of current DEXs. While a true DEX will inherently have different performance characteristics from a centralized exchange, we believe this problem can be overcome by a well-thought-out UI & UX. Switcheo's DEX will allow for **partial filling** of offers, **auto-retrying** of failed orders, and **order batching** within a single transaction. This provides the user the experience of using a traditional exchange while allowing them to remain in control of their funds through the Switcheo smart contract. Exchange of Tokens is done without delegating any key component (such as order matching) to an off-chain service where unseen shenanigans that compromise the integrity of the entire exchange may happen.

4.2 SMART CONTRACT SECURITY

As the security of a DEX is only as good as the security of its smart contract, we hope to run an aggressive **bug bounty campaign** over a minimum of 1 week on top of external audits, to minimize the possibility of any critical bugs in our smart contract. More details on this will be announced soon.

4.3 KYC / AML REQUIREMENTS

Many governments have KYC/AML laws and requirements, in addition to regulations for the trading of securities. We aim to implement D-KYC whitelists on our exchange so that users can trade on our exchange in compliance with the relevant legislations. Furthermore, we intend to monitor transactions on the Switcheo DEX for suspicious transactions, such that we can assist legal authorities in tracing and/or tracking illegal activities conducted through the blockchain.

4.4 LOW EXCHANGE VOLUME

We hope to overcome the problem of low liquidity / exchange volume through strong credibility, market presence and a state-of-the-art ease-of-use platform, such that using Switcheo's user experience is preferred even to popular centralized exchanges.

Archived copy · cryp2nova.com

5. NEO FRAMEWORK

5.1 GAP

NEO is a good first blockchain to enter the market with. The NEO blockchain has recently garnered international attention, and is growing at an enormous rate. Since the first ICO on NEO in October 2017 (Red Pulse, $RPX) there has been 6 more NEP-5 based ICOs with a total raised amount of $184,990,000, and 6 more ICOs planned in the near future[7]. However, there has yet to be an avenue where users may sell their NEP-5 tokens after they are made tradable without waiting for a centralised exchange to list them. This gives us a first-mover advantage in launching a DEX on NEO.

5.2 RESEARCH

The cumulative valuation of all ICO funding reached $3.775bn [6] in November 2017. 24 hour trading volume for all exchanges can reach billions of dollars for a single token or asset. Switcheo just needs to capture a small segment of this market to be profitable. For comparison, the combined trading volume for DEXs on Ethereum (EtherDelta + IDEX) is currently $6m. This is already a $60,000 daily revenue.

However, Switcheo's goal is not to compete with existing DEXs. We aim to compete head-to-head with centralized exchanges such as Binance and Kucoin, such that we may attain similar volumes to them. This is why Switcheo focuses fundamentally on 3 things:

1. Volume & Assets Available - Switcheo seeks to gain users by offering a viable option for buying / selling tokens that cannot be found elsewhere.
2. User Experience - By having an excellent UI/UX, retail traders are more likely stick to the platform, and hence more likely to grow its usage through word of mouth.
3. Scalability - At high transactions rates, DEXs perform suboptimally compared to centralized exchanges; Switcheo is commited to constantly refining, optimizing and improving its architecture to support increasing user loads to the best of its abilities.

6. SWITCHEO ARCHITECTURE

On centralized exchanges, most of the functional logic and data are performed and stored on their own servers. Switcheo's main operations, however, are mainly executed by a smart contract residing on NEO's decentralized blockchain.

There are 4 core components that make up the Switcheo DEX:

- A front facing user interface that interacts with the smart contract
- Custom blockchain nodes to log smart contract events and interactions
- Off-chain order history database and API
- Broker smart contract

6.1 FRONT-FACING USER INTERFACE (UI)

From the user's point of view, the Switcheo DEX operates almost identically to traditional exchanges that users are comfortable with. Where required however, we always remind users of the possible differences

Archived copy · cryp2nova.com

when performing an action. For example, trades are asynchronous, may fail and have to be re-submitted. Other differences include the fact that a user account is not required. We also “login” using the user’s wallet instead of an email-password pair, and can display their wallet balance, transaction history, etc. immediately.

Features:

- Market buy/sell
- Limit buy/sell
- Login through JSON Wallet, WIF, Private Key, Ledger
- Client-side matching and filling multiple offers within a single offer
- Automatic retry of failed fills
- Personal transaction history
- Trading charts (via tradingview)

The Switcheo UI is built on React.js.

6.2 CUSTOM BLOCKCHAIN NODE

The Switcheo smart contract will raise events when you perform certain actions using the user interface.

These events are emitted as smart contract event notifications which contain details of the interaction with the contract. Depending on the trigger of the event, the payload contains different information:

- `Created (Maker Address, Offer Hash, Offer Asset ID, Offer Amount, Want Asset ID, Want Amount)`
- `Filled (Filler Address, Offer Hash, Filled Amount, Offer Asset ID, Offer Amount, wanted asset id, wanted amount)`
- `Failed (Filler Address, Offer Hash)`
- `Cancelled (Canceller Address, Offer Hash)`
- `Withdrawal (Withdraw Address, Asset ID, Withdrawal Amount)`

We subscribe to these events using a full node. These events are stored and used for the presentation of auxiliary information (e.g. transaction history, trading chart) to improve the UI/UX of the user of the Switcheo UI. These events are informational and are not essential to the trading or operation of the Switcheo smart contract.

6.3 OFF-CHAIN ORDER HISTORY DATABASE AND API

We have developed an API which can retrieve and present data about orders and transactions on the Switcheo DEX in an easy-to-use JSON format. This API is used by the Switcheo UI and can be used by external applications which require the current and/or historical data from Switcheo (e.g. coinmarketcap).

6.4 SWITCHEO BROKER SMART CONTRACT

The Switcheo Broker Contract is the core engine that runs all asset swaps and handles deposit and withdrawal of assets through transaction invocations. An in depth description is given in the following section (Section 7).

Archived copy · cryp2nova.com

7. SWITCHEO BROKER SMART CONTRACT

The current smart contract is written in C# using the NEO framework. Any NEP-5 token and System Asset (NEO, GAS) are currently supported as trading pairs. The latest smart contract can be viewed here: https://github.com/ConjurTech/switcheo/blob/master/switcheo/BrokerContract.cs

7.1 OPERATIONS

There are 4 primary operations used for trading:

- **makeOffer**
  - This allows users to make an asset swap offer on the contract.
  - The params required are:
    - Script hash of the offer maker (invoking user)
    - Script hash of the asset being offered
    - Amount of asset being offered
    - Script hash of the asset wanted in return
    - Amount of asset being wanted
  - SystemAssets (NEO/GAS) must be attached if they are part of the fill.
  - Once invoked, the offered amount will be transferred to the smart contract, and the offer will be placed on the blockchain for anyone with the corresponding assets to fill.
- **fillOffer**
  - This allows users to fill an offer on the contract.
  - The params required are:
    - Script hash of the offer filler (invoking user)
    - Offer hash of the offer to be filled
    - Amount of offered asset that should be filled
  - SystemAssets (NEO/GAS) must be attached if they are part of the fill.
  - Once invoked, the offer corresponding to the correct offer will be filled. Partial filling is possible.
  - Amounts will be transferred to the maker and filler for withdrawal in a second transaction.
- **cancelOffer**
  - This allows a user to cancel a previous offer that has not been completely filled.
  - The params required are:
    - Offer hash to be cancelled
  - Once invoked, the offer will be cancelled and any remaining balance will be credited to the user balance for withdrawal in a second transaction.
- **withdrawAssets**
  - This allows users to withdraw their balance in the smart contract.
  - The params required (NEP-5) are:
    - Script hash of the user to withdraw balance from
    - Script hash of the asset to withdraw
    - Amount of asset to withdraw

Archived copy · cryp2nova.com

- For SystemAssets, params are not required, but the transaction must be invoked with a TransactionAttribute of Usage 0xd1 and Data 0x01. We chose an implementation which uses transaction attributes instead of "method arguments" to prevent double withdrawals before main net deployment.
- Our implementation currently does not allow a transfer trading of this balance and this operation must always be called to make use of the swapped asset.

There are other operations available for getting data about the Switcheo DEX, such as *getOffers* and *getExchangeRate*. There are currently 26 operations that can be performed on the Switcheo smart contract. We will detail the full ABI of the Switcheo smart contract at a later date.

7.2 OFFER LISTINGS

In order to find offers on the blockchain, list traversal can be used. By querying the contract's storage with a concatenation of the offered and wanted asset script hashes, the head of the list can be obtained.

This will give the offerHash of the latest offer on the trading pair. This allows the offer information to be queried and deserialized. Each offer contains the offerHash of the next offer. In this way, the list can be traversed entirely, and an order book can be displayed and/or cached.

8. SWITCHEO (SWH) TOKEN

Switcheo team will launch the token contract for Switcheo (SWH) Tokens no earlier than the 16 March 2018 on the NEO Blockchain as a NEP-5 Token.

1,000,000,000 SWH Tokens may be minted in total, and no additional tokens will be minted in future.

The allocations for SWH are as per follows:
20% (200,000,000 SWH Tokens) will be allocated to the Public Sale;
48.3% (483,000,000 SWH Tokens) have been allocated to Strategic Partners;
25% (250,000,000 SWH Tokens) will be reserved for the Switcheo Team to further incentivize development of the Switcheo DEX, and the tokens will be vest monthly on a 2 year schedule with a 3 month cliff; and
6.7% (67,000,000 SWH Tokens) will be reserved for Marketing Campaigns & Official Partnerships.

8.1 BASE TRADING PAIR

SWH Tokens will be added as a base pair while trading on the Switcheo DEX through the Switcheo UI.

8.2 SUBSIDISED TRADING FEES

SWH Tokens can be used to subsidise trading fees on the Switcheo DEX by 50%. Users may toggle this option in the trading UI. SWH Tokens will be burnt when they are used to pay trading fees.

Archived copy · cryp2nova.com

8.3 USED FOR CROSS SWAP

SWH Tokens will be used as the base token when doing cross swaps to other chains in future.

9. ROADMAP

Q4 2017 - Switcheo MVP Demo
Q1 2018 - Launch of Switcheo DEX for NEO, GAS & NEP-5
Q2 2018 - Launch of QRC20 trading
Q3 2018 - Launch of ERC20 trading
Q4 2018 - Cross-swap feature using SWH and Wanchain
2019 - Launch of trading for top 5 chains

10. DISCLAIMERS AND RISK STATEMENTS

By accessing the information set forth in this document or any part hereof, you represent and warrant to Switcheo that you accept the following:

10.1 PROHIBITION AGAINST VIEWING IN A RESTRICTED TERRITORY

It may be unlawful in certain jurisdictions for individuals, or certain categories of individuals in other jurisdictions, to view this document. An individual who wishes to view this document must first be satisfied that he or she is not subject to any local requirements that prohibits or restricts him or her from doing so. In particular, unless otherwise determined by Switcheo and permitted by the applicable law and regulations, it is not intended that any offering of the tokens mentioned in this document (the "Tokens") by Switcheo should be made, or any documentation be sent, directly or indirectly, in or into, countries where participating in Initial Coin Offerings are banned due to legal restrictions, and countries sanctioned by the US or countries considered as high risk and monitored by the Financial Action Task Force (“FATF”) (each, a “Restricted Territory”) and nor should it be accessed by any individual who is a national citizen or resident of a Restricted Territory, including corporations, partnerships, or other entities created, incorporated or organised in any such jurisdiction, unless they are exempted from the prohibition against participating in Initial Coin Offerings. Switcheo shall not be responsible for individuals who access this document from territories that prohibit such access or where any part of this document may be illegal. Such individuals do so at their own risk.

10.2 NO WARRANTY FOR INFORMATION PROVIDED IN THIS DOCUMENT

All information is provided without any warranties of any kind and Switcheo, its employees, officers and/or advisors make no representations and disclaim all express and implied warranties and conditions of any kind and each of Switcheo, its employees, officers and/or professional advisors assume no responsibility or liability to you or any third party for the consequence of relying on such information, errors or omissions in such information or any action resulting therefrom.

Archived copy · cryp2nova.com

The information set out in this document may contain statements that are deemed to be “forward-looking statements”. Such statements are prospective in nature and are not statements of historic facts. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “project”, “should”, “anticipate”, “believe”, “if”, “intend”, “may”, “plan”, “could”, “estimate”, “probable”, “expect”, “possible”, “would”, “will” or other similar terms. However, these terms are not exhaustive. Forward-looking statements inherently contain risks and uncertainties as they relate to events or circumstances in the unforeseeable future. Therefore, the information, opinions and forward-looking statements, including estimates and projections, in this document in respect of the anticipated roadmaps, development and projected terms and performance of the relevant entities, are selective and subject to adjustments, updates, expansions, revisions, independent verifications and amendments.

Switcheo is not making any representation or warranty or undertaking, including those in relation to the truth, accuracy and completeness of any of the information set out in this paper. Switcheo also expressly disclaims any obligation or undertaking to update or revise any forward-looking statements except to the extent required by law and neither Switcheo, its employees, officers or professional advisors make any assurance, representation or guarantee that any event referred to in a forward-looking statement will actually occur. Whilst Switcheo intends to achieve all the goals set out in this document, the goals may change or may not be achieved without any notice to you in case of unforeseen circumstances.

10.3 THIS DOCUMENT DOES NOT CONSTITUTE AN OFFER

This document is for information purposes only and does not constitute or form, and is not intended to be, an offer or solicitation of an offer to buy or sell, subscribe for, underwrite or purchase any form of investment or securities or other financial instruments, nor shall it or any part of it form the basis of, or be relied upon in any way in connection with, any contract or investment decision relating to the same.

10.4 THIS DOCUMENT DOES NOT CONSTITUTE ADVICE

The contents of this document do not constitute legal, financial, tax or other advice. You must conduct your own due diligence and ensure you comply with all local laws regarding cryptocurrency, tax, securities and other regulations in your jurisdiction. We encourage you to consult with the relevant professional advisors independently.

10.5 THIS DOCUMENT DOES NOT CONSTITUTE AN AGREEMENT

This document shall not be relied on to enter into any contract or to form the basis of any investment decision. Any agreement(s) between Switcheo and you are to be governed by a separate document (“Sale Document”). In the event of any inconsistency between this document and the Sale Document, the relevant Sale Document shall prevail.

10.6 THIS DOCUMENT IS NOT AN ADVERTISEMENT

This document is for general information purposes only and is not an advertisement, nor is it intended to be used to call for an offer on behalf of Switcheo. The distribution of this document may be restricted or prohibited by law or any regulatory authority in your jurisdiction. Recipients of this document should

Archived copy · cryp2nova.com

inform themselves of, and comply with, all such restrictions or prohibitions and Switcheo does not accept any liability to any person in relation thereto.

10.7 REGULATORY RISKS

The regulatory status of cryptographic tokens, including any digital currency, digital assets and blockchain applications is unclear or unsettled in many jurisdictions. The publication and dissemination of this document does not imply that it is compliant with any relevant laws, regulations and rules. This document has not been examined or approved by any regulatory authority. Where any relevant governmental authority makes changes to existing laws, regulations and/or rules, or where financial institutions make certain commercial decisions, it may have a material adverse effect and/or impair the ability of any relevant entity referred to in this document to function as intended, or at all.

10.8 OTHER DISCLAIMERS

There are risks involved in the technologies relating to the NEO Blockchain, Switcheo DEX, SWH Tokens, the Initial Coin Offering, and the Switcheo Smart Contract, and other blockchains, such as unforeseen bugs, security issues or disruptions. By way of the above and other factors not within our control, the entire sum used to purchase the SWH Tokens may be lost.

Despite our best efforts, Switcheo may not be able to execute or implement its goals, business strategies and plans.

There may be changes in political, social, economic and stock or cryptocurrency market conditions and/or that there is no or little acceptance/adoption of the Switcheo DEX and/or SWH Tokens, such that the Switcheo DEX and/or SWH Tokens become no longer commercially viable.

To the fullest extent possible, Switcheo shall not be liable for any responsibility, liability, claims, demands and/or damages (actual and consequential) of every kind and nature, known and unknown (including, but not limited to, claims of negligence), arising out of or related to any acceptance or reliance on the information set forth in this document by you.

Whilst we have made references to certain websites and links in this document, we did not seek further verification as to the accuracy, completeness, or timeliness of the information referred to in those websites and links.

The disclaimers set out in this document are not exhaustive and a more comprehensive list will be set out in other documents that may be published by Switcheo from time to time.

CRYP2NOVA

Archived copy · cryp2nova.com

REFERENCES

[1] https://cityofzion.io/dapps/1
[2] https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html
[3] http://bitcoinist.com/coinbase-missing-funds-legal-action/
[4] https://en.wikipedia.org/wiki/Bitfinex_hack
[5]https://coin.red-pulse.com/
[6] https://www.coindesk.com/ico-tracker/
[7] https://stateofneo.com/projects/

Archived copy · cryp2nova.com