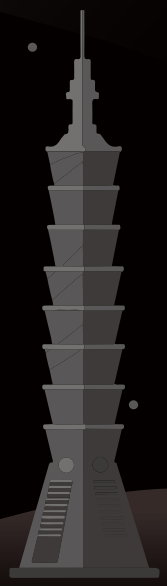
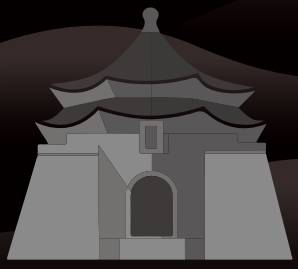
JOYSO

WHITE PAPPER

World's First
Hybrid Decentralized Exchange





t.me/joyso_io twitter.com/joyso_io JOYSO.io

Contents

Executive Summary

JOYSO suggests a hybrid design for token trading, combining the advantages of a centralized exchange - fast and fully-featured - with the advantages of a decentralized exchange - improved security and privacy.
This hybrid exchange (HEX), able to handle all ERC20-compatible tokens, eliminates the need to trust a central exchange with your private key or personal information, reducing to a historical minimum any opportunities for hacking. It takes order placement and order matching off-chain, substantially improving the user experience compared to decentralized exchanges. In brief, the benefits and innovations of the JOYSO model are these:

- All orders are limit orders, giving users the best possible price.
- Smart matching is done off-chain, providing fast processing and one-to-many matches.
- Smart matching eliminates security issues like front-running and makes arbitrage by the exchange transparent.
- One-to-many matches merge multiple orders into one transaction, so gas fees are substantially lower than in first generation decentralized exchanges.
- The exchange cannot alter the balance in a user's account, and has no access to the user's assets.
- Users do not need to log on to a website; they just sign the bid or ask using their own wallet and send ether directly to the smart contract.
- Users have the ability to cancel transactions up until they are matched and can even lock the smart contract themselves.
- Completed trades are published on the blockchain in a transparent, traceable way.

Compared to its competition, JOYSO has a low cost structure and offers users lower transaction and settlement costs.

The marketing strategy includes aggressive pricing (including free listing for ICOs) and professional, targeted digital marketing. The development team comprises eleven people and is based in Taiwan. It has deep connections with the Chinese-speaking Bitcoin and Ethereum communities.
Wallet support currently exists for Metamask and Ledger Nano S. The project is currently in alpha and a beta release is scheduled for June 2018. Proof of concept has been done on all principal functions and the team is ready to migrate the system to the Ethereum testnet. Margin trading and cross-exchange are part of the second phase launch.

200 million JOY tokens will be issued in total; 100 million of them in an ICO event commencing March 1st, 2018.

CEX, DEX and HEX

Although efficient and fast, the centralized exchange(CEX) is intrinsically vulnerable to hacking, denial of service attacks and fraudulent management. Losses to investors and companies amount to around a billion U.S. dollars in 2017 alone.

The risks of centrally controlled exchanges are not going away and movement towards the decentralization of trading is inexorable.
However, prototype decentralized exchanges (DEX) have so far not delivered a satisfactory user experience, for three reasons.

The feature set of DEX has not matched that of established CEX. For example, limit orders are generally not supported.

Secondly, the blockchain is an inefficient architecture for the rapid, iterative processes required by a trading environment - cancellations, price queries, multiple bids and asks, etc.

Blockchains independently verify and process every transaction in every distributed node of the network which causes slow processing times. That latency is not just an inconvenience, it introduces opportunities for market manipulation by miners, exchanges and traders.

Thirdly, conducting all trading interactions on the blockchain is excessively expensive in terms of transaction fees. Every order, modification and cancellation incurs gas fees.

For these reasons - it's clear to most informed observers that a hybrid solution is the way forward.

An optimal HEX design would be a decentralized architecture in which users control funds and a centralized database that dynamically matches market transactions. Only when a deal is done and tokens are confirmed available, would the transaction be published on the blockchain. Users would not relinquish control of their assets and would have the benefit of a dynamic market where trades are processed sequentially, in near real-time.

When trades are broadcast to the Ethereum blockchain they would be transparent and traceable, making market manipulation by the exchange much easier to detect than is the case with CEX.

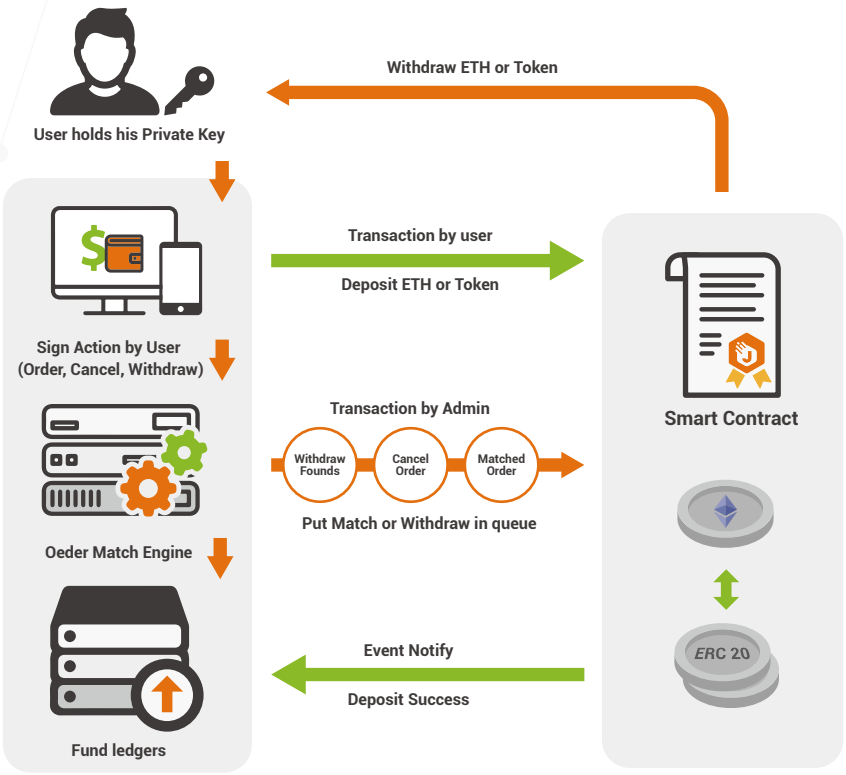
Rather than an on-chain order book, which is slow and incurs substantial gas fees, a HEX would centralize matching. Automated matching of orders is common in centralized exchanges but is not practical in an on-chain environment.

The HEX would then be able to replicate the feature set of large centralized exchanges.
For example, it would permit a single order to have multiple executions - multiple buy or sell orders in a single trade. The unfulfilled portion of an order would automatically be re-categorized as a new, smaller orde. In addition to the efficiency dividend, this would lessen the impact of exchanges and large ICOs on overall network performance.

Due to its distributed nature, HEX does not require a customer to log in, supply any customer details or temporarily surrender title to a deposited sum of money. In a HEX, ownership passes directly to the purchaser. The exchange facilitates a transaction but has no title or access to the tokens being exchanged.

Settlement can then be done on-chain with smart contracts that cannot be altered or interfered with. The smart contracts act as a verifiable, open source trust engine.
This is the system that JOYSO has developed and is bringing to the Ethereum blockchain.

JOYSO Architecture



JOYSO is a hybrid architecture which combines the transaction speed of off-chain order matching (as used in a centralized design) with the privacy and security of smart contracts in a decentralized design.

All JOYSO orders are limit orders; i.e. an order to buy or sell a stock at a specific price or better.

There are three main processes:

1. A trader sends instructions to JOYSO (deposit, order, cancel, etc) using a web interface and cryptographically signs it. They send tokens from their wallet directly to the smart contract.

2. The matching of orders is done off-chain by the JOYSO Order Match Engin. One-to-many matches ensures purchasers get the best price possible. Matching takes place on JOYSO servers and are visible on the browser in real time. Ordersare processed on a first-in, first out basis and matched orders are broadcast in sequence on the Ethereum blockchain. The matching algorithm is not open source code, akin to centralized exchanges. However, if JOYSO were to manipulate the sequence of the broadcast in order to conduct arbitrage for its own benefit, the changed order would be visible on the web site, revealing the manipulation.

3. The smart contract verifies the user signatures and publishes the transaction on the blockchain. Until the match is made, users have the ability to lock the smart contract and request a transaction cancellation. Later, they can withdraw funds directly if necessary.

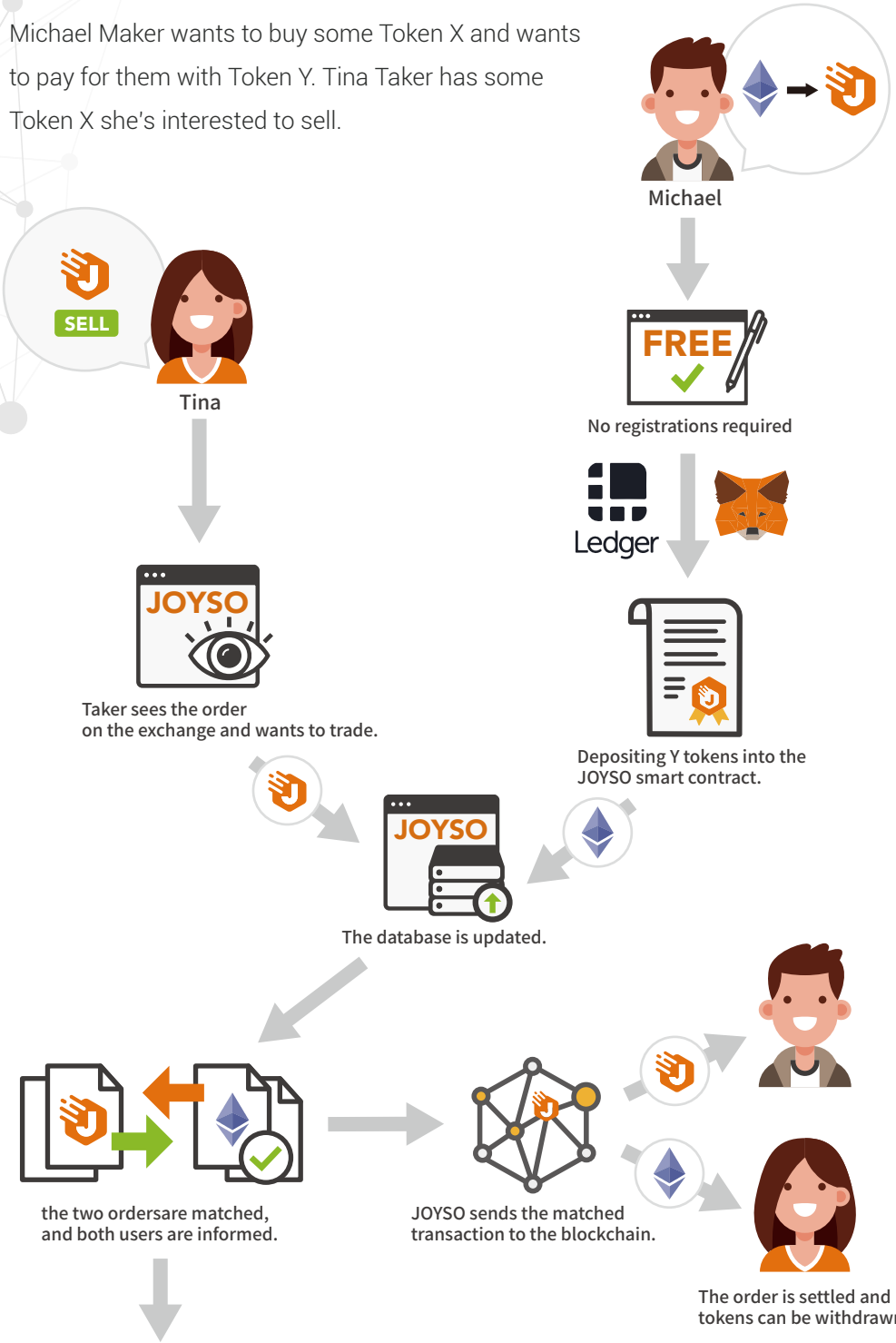
JOYSO Administration can't modify the content of the smart contract once the transaction is published, so have no access to the user's assets. Since users have signed the transactions themselves, and the blockchain is an open ledger, all trades are transparent and traceable.

No-one can alter the user's balance in a JOYSO contract without the user's signture. And the smart contracts, which are open source, can not publish a trade to the blockchain unless it contains the private key of the JOYSO Admin.

The smart contact that sends the transaction acts as the 'trust machine', replacing the audit normally done by a centralized exchange with a transaction verifiable on etherscan and with open source code posted on Github..

Example of a Transation on JOYSO

Michael Maker wants to buy some Token X and wants to pay for them with Token Y. Tina Taker has some Token X she's interested to sell.



Smart Matching

Compared to the one-to-one matching of orders used in most decentralized exchanges, users will prefer JOYSO smart matching.

Tina has placed an order. She wants to sell her 100 Y tokens and seeks 10 X tokens in exchange. If there are matching orders in the system, she may not have to spend all of her 100 tokens. Smart matching will connect her with the best offer listed for 10 X tokens.

In a one-to-one system she could be matched with any person wanting 100 Y tokens. If the JOYSO database contains no matching order, Tina's sell order for 100 Y tokens automatically becomes an open buy order for 10 X tokens and has the possibility of earning over 100 Y tokens in a future trade.

The smart contract enforces rules that deliver results as good or better than what the user has requested.

JOY Token

It is planned that 200 million JOY tokens will be generated and distributed as follows:

50% Crowdsale ICO
25% Private placement
25% JOYSO team

Using the JOY token will entitle users to a 50% transaction fee discount. The discount does not apply to gas fees.

Token holders will have the right to participate in various campaign activities hosted by JOYSO. This may include discussions regarding which tokens shall be listed on the exchange.

Advertisers can also use the token to earn discounts. Other benefits for using JOY will be announced in time.

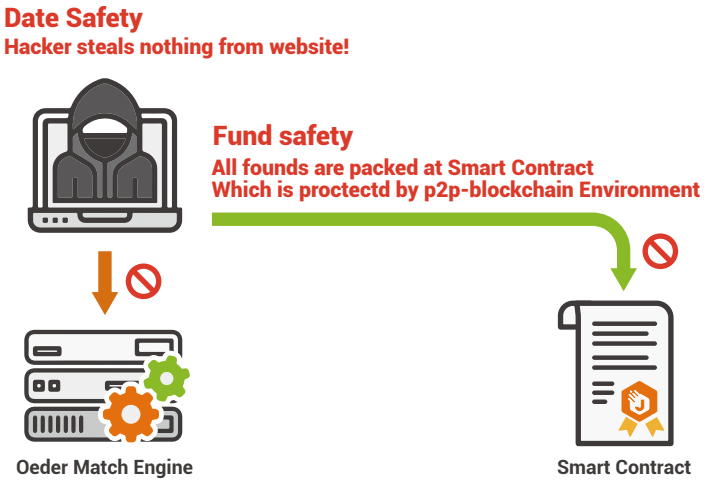
See the Token Sale section for sale specifics.

Security Issues

Decentralized and hybrid exchanges must rely on secure wallets to ensure safe digital signing of their clients' instructions. Initially, JOYSO will support MetaMask and Ledger Nano S; two wallets used widely and well-regarded in the crypto community.

Once the order is signed, it is sent to the Order Matching Engine. Then the JOYSO Admin will send the matched order to the smart contract, to verify the order and settle funds.

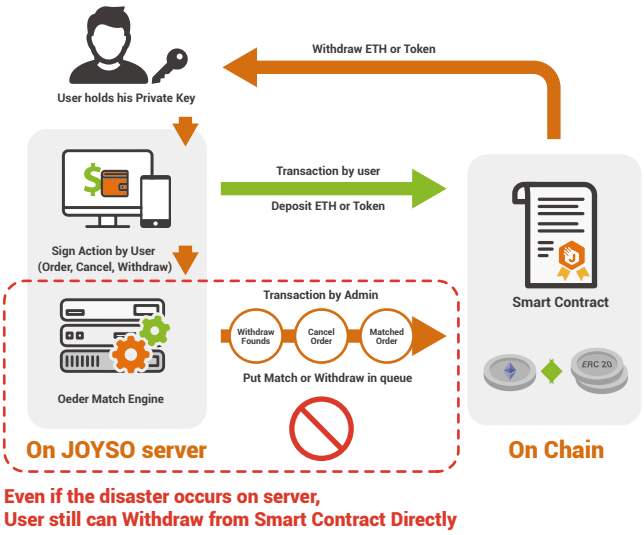
Tamper Resistance



Even if a hacker gained control of the JOYSO website, without the private key of the JOYSO Admin, the smart contract would not execute. The contract would detect an unverified admin account and the fraudulent transaction would fail.

In the event of the JOYSO Admin account private key being stolen, control can be quickly regained with multi-signature authorizations.

Disaster Recovery



A user can cancel orders he has previously signed with the assistance of JOYSO Administration. If the problem was with the JOYSO server, the user could lock his account for a period of time, then withdraw funds directly from the smart contract without JOYSO administrative involvement.

Threats

The balance of this section looks at the JOYSO architecture with respect to security threats.

1. JOYSO token contract

The token follows closely the ERC20 token standard and uses code based on OpenZeppelin, with these amendments:

A lock has been added to prevent malevolent token transfer. An unlock call is required from the contract owner to transfer the locked token.

The owner will initially be set to JOYSOWallet during the distribution of pre-sale tokens. Then manually, with the multiSig wallet, the owner will be changed to the ICO contract.

Now the tokens can only be distributed as specified in the contract's code. Once the ICO has ended, the contract will call the unlock function to release the token to the user.

The lock can only be set to unlock once; it cannot be reset to 'lock'. No outside calls are permitted in the token contract, so the possibility of a reentrancy attack does not arise.

The unlock function can be called by any user and is not derived from library code so additional testing is required.

2. Crowdsale contract

This is based on the OpenZeppelin crowdsale contract.

A release function is able to unlock the JOY token contract. This function can be called by JOYSO Admin after the ICO has ended. If for some reason Administration does not trigger the release, the system allows for any other user to do so after a few days.

The funds will be sent directly to JOYSOWallet, so no ether can be locked in the contract. The outside calls are (a) the unlock function and (b) transfer ether to JOYSOWallet. Both addresses are controlled by JOYSO, so again, no possibility of a reentrancy attack.

3. JOYSO contract

This is more complex than average contracts so we will have it independently audited until we are satisfied it is reliable.

We also plan multiple scenario unit tests and function tests to give the broadest possible test coverage. JOYSO uses the library provided by OpenZeppelin; related libraries include SafeMath, Ownable, and ERC20 token contracts are used.

Results generated by the Order Match Engine only update the balance status in the JOYSO contract. Only normal users are able to interact with the smart contract and signatures are required for any action. At present it is not possible to call a smart contract, so there's no risk of a reentrancy attack. Further, we have limited the gas that external calls can use. An illegal execution would cause an 'out of gas' error that stops the transaction.

Cancellations of orders can be seen on the blockchain. If a user can not see a cancellation or has reason for concern, they have the ability to withdraw funds without our permission.

JOYSO is not vulnerable to front-running attacks by miners or traders because user gets the returned results in a second, as per the CEX experience. Even though JOYSO could theoretically front-run users by itself, users could detect that orders were not in sequence.

4. Multi-sig wallet

We use the wallet provided by the Gnosis team, unchanged. The contract is widely used by many well-known blockchain financial institutions including Bancor and has no dependencies on other libraries. For this reasons it can not be frozen in the way the Parity wallet was.

Governance

Legally, we are constituted in Taiwan, where crypto-currency is regarded as a commodity, not money.
We are aware of restrictions that apply to ICOs in certain countries and will prevent IP addresses there accessing those tokens in the exchange.
We have no involvement with fiat currencies so do not envisage any governance complications in that regard.
In terms of operational governance, much of this is handled by the JOYSO Aadmin account.

- It sends the matched order automatically to the smart contract, confirming the transaction and settling the funds of each counterparty.

- It broadcasts operational status changes; for example, the launch of a new function, the blockchain's current traffic load, system maintenance requirements, etc.

- It is the way we manage the deployment of new smart contracts, notifying users to withdraw funds and tokens from the old contract in a timely manner.

Code Quality and Testing

JOYSO use both behavior-driven development and test-driven development to ensure product security and a quality user experience. We use the Zeppelin Solidity framework to provide patterns for secure code that can be reused without duplication.

Performance testing is currently underway for the Order Matching Engine and trading engine. Immediately after the ICO, we will migrate these and the smart contracts to the Ropsten Test Network so that we can prove all functions executable.

We have done proof-of-concept on the testnet for deposits, withdrawals, order matching and order cancellations. Server-side is operational. We are currently testing the server and working on further reducing gas costs.

There are two arms to our server security; internal server-side testing and auditing done in the bounty program (to commence after the ICO). Face-to-face user testing and independent auditing will be done before the application is migrated to the mainnet.

Business model

Trading fee discount

Income will be generated from trading fees in ether or JOY effective from the beta launch; May 2018. These will be set around 0.1% for order makers and 0.2% for order takers.

Our price strategy is to attract users with a 50% discount for JOY token use. We will generate transactions and advertising by offering free and frictionless listings to ICOs.

Advertising on JOYSO through the JOYSELECT program will also be competitive, with a 50% discount for ICOs paying with JOY.

Token reduction plan

Each quarter, we will burn JOY tokens equal to 50% of our net profits, until 50% of the total supply (100 million JOY) are destroyed. The process will be announced on the blockchain. Eventually we will destroy 100 million JOY tokens in total, leaving 100 million JOY tokens.

This will be our commitment to our investors.

In the second phase

When available as part of our second phase, we expect margin trading to be very attractive to users, as the collateral required for trading using the JOY token will be lowern than with ether.

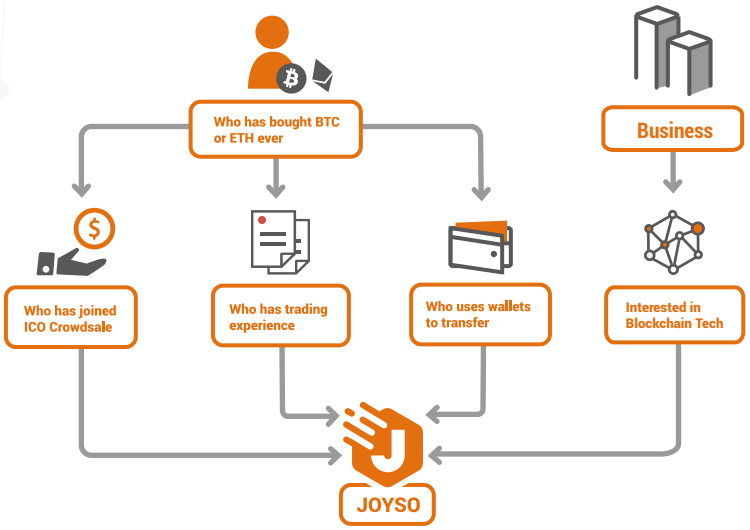
Compared to centralized exchanges, we offer reduced settlement costs and low-cost integration with wallets due to efficiencies in smart contracts and block-chain. We expect to generate increasing business as word spreads through the community.

The efficiencies of the HEX exchange structure create a low cost operation with an attractive feature set. Because we don't store the private keys of users, we don't require expensive hardware and software systems to segregate/protect them. We mitigate the higher gas fees normally associated with decentralized exchanges by zipping the input arguments and optimizing the gas consumption.

Marketing Plan

Target Market

People between the ages of 18 to 45, who are interested in digital currency trading, fintech investment opportunities and hungry for blockchain knowledge.
Businesses that see a need to improve operational processes with the use of blockchain technology.



Target Audience: Market segmentation and the user experience journey

Positioning

1. JOYSO is a hybrid exchange (a HEX). It offers traders the speed and features of a centralized exchange with the privacy and security of a decentralized network.
2. JOYSO is a technology savvy start up that helps to build technology utlizing decentralized application and smart contracts.

Communication points

For CEX users:

- Do you really want to give an exchange your private keys?
- Do you really want to let an exchange fully control your funds?
- USD$1B in crypto hacked/stolen in 2017

For DEX users:

- Why is this so difficult?
- Why is this so slow?
- Why so much gas?

Communication points

For Businesses :

- How can we improve current processes?
- How do we save time?
- How do we simplify approaches?

Channels

Based on our market research and numbers, we will focus activities primarily on Taiwan and Asian countries with English as a primary language. Our secondary markets will cover global advocate countries such as Canada, the United States of America, etc.

Aside to targeting countries, our strong connections with Bitcoin adopters in China and Singapore, this can be leverage to give outreach support to communities looking to understand and trade with cryptocurrency.

Marketing strategies

Bull market

During a bull market situation, we will proceed global advocate markets with digital marketing and roadshows and conferences to promote our services and vie for branding exposure in the marketplace.

Bear market

We will be focusing our energy on the educating and growing new user base through community events and barter partnerships to shape branding, communications and comunity growth.

Advertising

Our advertising channels will cover mainly on digital advertising, commmunity seeding and partnerships. Using in-house and reward schemes for content contributors to portray thought leadership approach to educate and inform old/new users in the marketplace.

Community building

We will work with local event/meet up organisers to co-run local events while we will attend selected conferences globally to raise our profile and introduce our expertise. We also run campaigns on social media platforms such as Facebook to growth the user base.

The Team

The team has over 20 employees, JOYSO is developed out of Consensus Innovation Ltd, a blockchain innovation incubator in Taiwan with a globally reach. Consensus has worked on copyrights in music, financial projects and blockchain projects including Dodoker, Tokenlab, CPChain, Muzeum and NAS-JOYSO on Nebulas chain.

TomSoong
CEO

Tom is responsible for the overall management of Joyso, the world's first Hybrid-Decentralized Exchange after 5 years of experience in the Blockchain industry. His deep commitment to improve the Blockchain industry had him supervised the development of the world's first 28nm Bitcoin mining chip and brought to market the 40nm Litecoin mining chip. Tom also contributes himself to the Blockchain community as a Blockchain advisor to ITRI, one of the world's leading technology research and development institution and is the administrator of Bitcoin Chinese Community and Taipei Ethereum Meetup. Tom holds a Master Degree in Electrical and Electronics Engineering from National Tsin Hua University in Taiwan.

Taka Kao
COO

Taka is responsible for the operation and administration of JOYSO, the world's first Hybrid Decentralized Exchange.
He had over 10 years of experience as a Technical Manager at the Industrial Technology Research Institute (ITRI) of Taiwan where he managed a diverse range of digital and big data projects that includes Blockchain technology in the public sector. He was also the Technical Architecture contributor of the Dodoker project, blockchain-based crowdfunding platform, and the principal organizer of the Taiwan Blockchain Summits in 2016 and 2017. Taka graduated with a Bachelor and Master of Sciences in Mechanical Engineering from National Taiwan University.

Will Hsieh
CTO

Will is responsible for the technical development of JOYSO decentralized exchange platform. Before Joyso, he was the key contributor to Gcoin, an first Taiwan approved enterprise-level distributed blockchain infrastructure and had collaborated in creating decentralised applications for LogoVote, ticket contract for an Ethereum conference, Dodoker charity crowdfunding platform and Muzeum's blockchain-based creative industry protocols. He is also the joint operating officer for the Ethereum Taipei Meetup community, lectured several Smart Contract course and an advisor to several Blockchain projects. Will graduate with a Masters of Computer Science from the National Taiwan University.

Chen Yi Cyuan
Chief Architect

Yi-Cyuan is responsible for the full stack work at JOYSO. He is a full-stack software engineer with over ten years' experience in software development, a regular contributor to many open source projects on GitHub, including js-sha3. His employment history includes front and back end development, as well as settlement and clearing at Titansoft Ltd., a global online gambling company with over 100,000 concurrent users. He is responsible for the full stack work at JOYSO. Yi-Cyuan holds a Master Degree in Computer Science from National Central University of Taiwan.

Gerald Chan
Marketing Director

Gerald is responsible for Branding, Marketing and Public Relations for JOYSO. He has over 12 years of experience in marketing in several industries that include entertainment, high valuable logistics, property and investment. He had working experiences in Singapore, Hong Kong and currently based in Taipei, Taiwan. He graduated with a Bachelor of Arts in Mass Communications majoring in Multimedia from Curtin University of Technology of Western Australia.

Partner

Roadmap

Project start
OCTOBER, 2017

ICO start
MARCH, 2018

Prototype release on testnet
APRIL, 2018

Trading API
DECEMBER, 2018

Mobile version
SEPTEMBER, 2018

JOYSO launch
MAY, 2018

Margin trade
MARCH, 2019

Off-chain payment integration
JUNE, 2019

Mobile payment and wallet
SEPTEMBER, 2019

Application Of Funds

Post ICO, funds will be applied as follows:

	Application	Principal tasks
35%	Target Market	Development of trading engine, order match engine, smart contracts, migration to main net, security protocols, back-end development, wallet integrations, front-end development, mobile development, testing, margin trading support, stable coin(Dai) testing, cross- centralized exchange development.
20%	Marketing	Targeted advertising such as google research, Attending, exhibiting, sponsoring of conferences and events Social media platform development, content creation video community development and engagement on prominent platforms Partnership promotion and offers.
15%	Operations	DevOps environment, status monitoring and reporting, system deployment and backup, load balance, performance tuning, issue tracking. Customer services and support team, token auditing and listing, market price watch and trading fee updating, Funds settlement and operating report.

Application	Principal tasks
10% **Legal compliance**	Prepare for new regulations due to the rapid changes in the digitalworld.
10% **Security Bounty**	To facilitate independent, low-cost auditing of JOYSO systems to reach the security level of tamper resistance and disaster recovery.
10% **Team Reward**	To encourage and inspire team growth.

THANK YOU!

For information please contact us at
info **@joyso.io**
or
join our Telegram group at
t.me/joyso_io