TomoChain Lab Pte. Ltd.
219 Trung Kinh, Hanoi, Vietnam
10 Anson Road #22-15 International Plaza, Singapore
Shotoku Bldg. 7F, 3-8-9 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan

TomoX: TomoChain Proposal for a Relayer-Masternode Decentralized Exchange Protocol

Preliminary draft, comments are welcomed
Long Vuong at long@tomochain.com

PREFACE **2**
TomoChain's Vision and mission 2
Scope 2

INTRODUCTION **3**

TOMOX: TOMOCHAIN DECENTRALIZED EXCHANGE PROTOCOL **4**
Overview of TomoX's usage flow 4
TomoDEX Web 5
Order Serializer 6
Tomo Swarm 6
Order deserializer 6
Decentralized order book database 6
Matching engine 7
Order processor 7
Transaction processor 8
Order settlement smart contract 8

RELAYER AND MASTERNODES **8**
Why do we need relayers? 9
Advantages of Relayer-Masternode architecture 9
Incentives for Relayer operators 10

TOMOX PROTOCOL SUMMARY **10**

PREFACE

TomoChain’s Vision and Mission

Our mission is to be a leading force in building the Internet of Value and its infrastructure. We are working to create an alternative, scalable financial system which is more secure, transparent, efficient, inclusive and equitable for everyone.

TomoChain relies on a system of 150 Masternodes with Proof of Stake Voting (PoSV) consensus that can support near-zero fees and 2-second transaction confirmation times. Security, stability and chain finality are guaranteed via novel techniques such as double validation, staking via smart-contracts and "true" randomization processes.

TomoChain supports all EVM-compatible smart-contracts, protocols, and atomic cross-chain token transfers. New scaling techniques such as sharding, EVM parallelisation, private-chain generation, hardware integration will be continuously researched and incorporated into TomoChain's Masternode architecture which will be an ideal scalable smart-contract public blockchain for decentralized apps, token issuances and token integration for small and big businesses.

Scope

This document describes TomoChain’s initial design draft for TomoX - a secure and efficient relayer-masternode decentralized exchange protocol based on the TomoChain blockchain infrastructure.

INTRODUCTION

Cryptocurrency exchanges have become an indispensable part of cryptocurrency and blockchain ecosystems, especially since the rise of major cryptocurrencies such as BTC and ETH and the increasing adoption of decentralized applications (Dapps). Cryptocurrency exchanges provide liquidity solutions for users to exchange their cryptocurrencies for other cryptocurrencies, which eventually allows them to access any decentralized applications. In general, cryptocurrency exchanges can be classified as centralized exchanges (CEX) or decentralized exchanges (DEX).

Early blockchain-based developed cryptocurrencies such as Bitcoin and Dash have become more widely used thanks to the help and the wide usage of centralized exchanges such as Coinbase, Bitfinex and Binance. The advantages of these exchanges are their user friendly interface and high performance that allow users to instantly transact/exchange cryptocurrencies with anyone on the exchange. Furthermore, because of high trade volumes and liquidity of centralized exchanges, to this point they have attracted more users than decentralized exchanges.

With the wider use of CEXs, their security and safety have become an increasingly hot topic of discussion. It is worth highlighting that some of the largest hacks in the history of cryptocurrencies have been through centralized exchanges such as MtGox and Bitfinex - where 850,000 BTC in 2014 and 120,000 BTC in 2016, respectively, were stolen. In short, there has been a tremendous amount of money stolen from CEXs. One of the reasons for these hacks has been centralized exchanges failing to protect the private keys of wallets that users had deposited their cryptocurrency into. Once a user deposits their cryptocurrency into a centralized exchange wallet, the user no longer has control of the wallet and must put their trust in this third party. However, this trust model seems to directly contradict blockchain's ideology of eliminating the middleman.

At TomoChain, our vision is that *decentralized exchanges (DEXs) will be the future of cryptocurrency exchanges*. DEXs allow users to control their assets while transacting, thus making them significantly safer and more secure than CEXs. The majority of currently deployed DEXs are based on Ethereum smart contracts and are mostly used for trading between Ethereum and ERC20-based standard tokens. The most widely used DEX based on Ethereum is IDEX, where most ERC20 issued tokens can be traded.

At TomoChain, with our current masternode architecture and ideology of the token economy, our decentralized exchange will become a very important part of TomoChain's ecosystem and TomoChain's masternode-based economy.

In this paper, we describe the TomoX Protocol - TomoChain's proposal for a secure and efficient relayer-masternode decentralized cryptocurrency exchange protocol. Compared to the current state of the art DEX architecture, TomoX Protocol has the following unique features:

- **Blockchain core layer-integrated DEX**: All current Ethereum-based DEXs are layer 2 solutions which rely on smart contracts with their matching engine combined with either off-chain or on-chain settlement. In contrast, TomoX will be integrated into the core blockchain layer where the high performance and fast confirmation time properties of our Proof-of-Stake Voting (PoSV) consensus will be beneficial.
- **Decentralized order book and matching engine**: Most current decentralized exchanges store their order books in centralized servers where the matching engines scan over the orders in order to execute trades. In contrast, TomoX aims to be a fully decentralized exchange protocol and rely on storing all trades on the chain, which are verified by every masternode, thus totally decentralizing the protocol. The masternodes will provide infrastructure and computation for order matching and execution.
- **Relayer-masternode architecture**: Building a decentralized exchange and providing traders with a significant liquidity pool are difficult and expensive tasks. In addition, an exchange trading thousands of tokens can be a source of confusion for traders with the potential to lose focus in some tokens of interest. TomoX has therefore been built to solve these issues by providing a relayer-masternode architecture. Relayers will have the responsibility of increasing trading liquidity on their exchanges for specific tokens.

TOMOX: TOMOCHAIN DECENTRALIZED EXCHANGE PROTOCOL

The uniqueness of TomoX Protocol stems from the way it is integrated into TomoChain's masternode architecture. In addition to executing and verifying transactions from users, masternodes will also execute the functions of TomoX. The following figure shows how the TomoX Protocol integrates the transaction processor into the current masternode architecture.

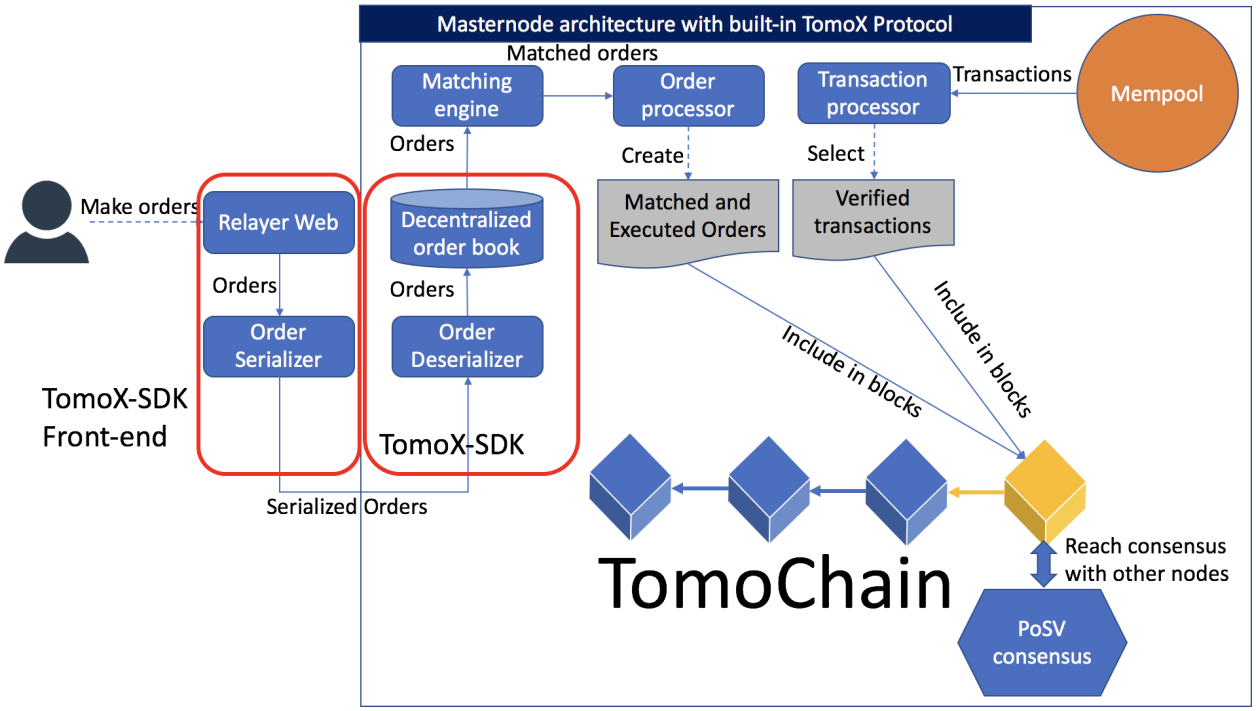
Overview of TomoX's usage flow

A user makes an exchange order through TomoDEX Web (part of the TomoDEX relayer detailed later). The order-related data is then serialized and sent to TomoX-SDK, a decentralized storage system. TomoX-SDK subsequently broadcasts the order to all masternodes in the system. After the serialized order data is received and read from Tomo Swarm, it is deserialized and stored in a structured way within a decentralized order book.

A matching engine then matches buy and sell orders to be executed, and the order processor then executes the matched orders. For each matched order pair, the order processor directly

changes the TOMO/token balance of the corresponding buyer and seller. This change will then be synchronized with all other masternodes through PoSV consensus. Afterwards, a settlement transaction is created and sent to a settlement smart contract that is deployed on TomoChain.

Each masternode takes turns executing matched orders based on the PoSV consensus. The masternode which is selected to create a block in a slot is responsible for executing the decentralized exchange functions within that slot.



User transactions coming to the transaction pool (mempool) of a masternode are processed by the transaction processor of the masternode. The processed transactions, together with the verified and executed trade orders, are then included in a newly created block. This new block is then broadcast to all masternodes in the network to reach the network consensus following the PoSV protocol.

The history of all orders will be persistently stored on the chain and shown to users through TomoScan in order to ensure the transparency of exchanges.

Relayer Web

Relayer Web provides an intuitive and optimal user interface for users to use the exchange functionalities. More importantly, users do not need to deposit any tokens to a centralized server, thus maintaining total control over their assets. As in any existing exchange, there are two types of actors:

- Maker: A market maker is someone who provides liquidity to the market by placing limit orders on the order book. Without limit orders sitting on the books, the price of cryptocurrencies would swing around wildly as exchanges try to match buy and sell orders.
- Taker: A taker is someone who takes liquidity (buys/sells from a limit order) from the exchange.

A maker order has to wait to be matched by either a taker order or by the matching engine. A taker order, on the other hand, does not need to go onto a matching engine, but is instead immediately matched with a maker order.

TomoX integrates these two standard actors. Furthermore, because of the difference in their roles, trading fees for makers are lower than those of takers.

For an order to be valid, it must be signed by a user using a private key associated with the user's wallet address. Once an order is sent, a cryptographic hash of the order's data is returned back to users' wallet so that all historical and pending orders can be traced back by using the orders' hash and Tomo Swarm. Users can also cancel a pending order without paying any fees.

Order Serializer

Structured orders made by users through Relayer Web are serialized into byte streams and sent to TomoX-SDK module of masternode, which is responsible for interacting with users and storing trading orders in a decentralized storage system. Serializing data to transfer over the Internet is quite common in today's applications.

TomoX-SDK

As opposed to most existing semi-decentralized exchanges, such as IDEX, where orders are saved in a centralized server, TomoX provides a decentralized order book by requiring all masternodes to store all pending orders in their local storage. TomoX-SDK of masternodes is run by all masternodes and candidates of the system. Any order broadcast to a masternode will be quickly propagated to all other masternodes.

- **Order deserializer**: Order deserializer is the opposite in semantics to Order serializer. Specifically, orders stored in byte streams in TomoX-SDK are deserialized into structured data, which are then saved to the decentralized order book database.
- **Decentralized order book database**: TomoX does not only provide a means for decentralizing order matching and execution, but also offers a decentralized order book. A decentralized order book stores exchange orders in a structured way (i.e. in relational or key-value database). Each masternode has a copy of the order book and this copy is

off-chain. More importantly, attempting to replicate the orders across so many masternodes makes it improbable to attack or corrupt the order book.

Matching engine

TomoX provides an off-chain matching engine, which is a common technique for increasing the performance in most existing DEXs built upon Ethereum. One of the most significant advantages of CEX features compared to DEXs is **performance**: a taker can trade instantly with an existing maker order and canceling a pending order is free. This is because all heavy operations such as order matching and execution are done in a centralized way.

TomoX is a unique combination of on-chain matching, a decentralized order book database, PoSV consensus and exchange integration. With this unique combination, TomoX's order confirmation will be almost instant, just as is provided by TomoChain's PoSV.

Generally speaking, for each trading pair TOMO/TokenX, the matching engine matches a buy order and a sell order with compatible price as follows:

- Maker-taker matching: A maker-taker order pair is immediately matched if both the taker and matcher order are available. If there are multiple taker orders targeted at the same maker order, a first-in first-out strategy will be used.
- Maker-maker matching: A buy order and a sell order are matched with each other if the maximum price of the buy order matches or exceeds the minimum price of the sell order.

The output of the matching engine is a set of pairs of orders, or set of trades that will be executed by the order processor.

Order processor

As previously described, and unlike most existing DEXs (i.e. for Ethereum) which are Layer 2 solutions, TomoX is directly integrated into the core consensus layer. Instead of relying on smart contracts, the order processor, which is integrated into the core TomoChain layer, can directly change the TOMO and TokenX balance of the buyer and seller.

All tokens issued on TomoChain will conform to certain standards. Initially, TomoX will support TRC21 tokens. TRC21 is an extension of the ERC20 token standard of TomoChain allowing to pay transaction fees in the token itself. (For more information about TRC21, readers are recommended to refer to TRC21 standard and TomoZ protocol). More standards will be gradually integrated into TomoX. In addition, TomoChain also provide token templates along with token standards in order for business makers and start-ups to easily raise funds and issue tokens for their projects.

All trading orders verified and executed by the order processor are included in a block, which is then propagated to the masternode network. All other masternodes will then verify those orders similar to verifying normal transactions.

Transaction processor

Transaction processor is the main component of TomoChain's masternodes in charge of verifying transactions to include in a block. Normal transactions (TOMO transfer or smart contract call transaction) come to the transaction pool, and are then read by the Transaction processor. All processed transactions are then added to a block, which is verified by the network through PoSV (this is what is already being done in TomoChain at the moment).

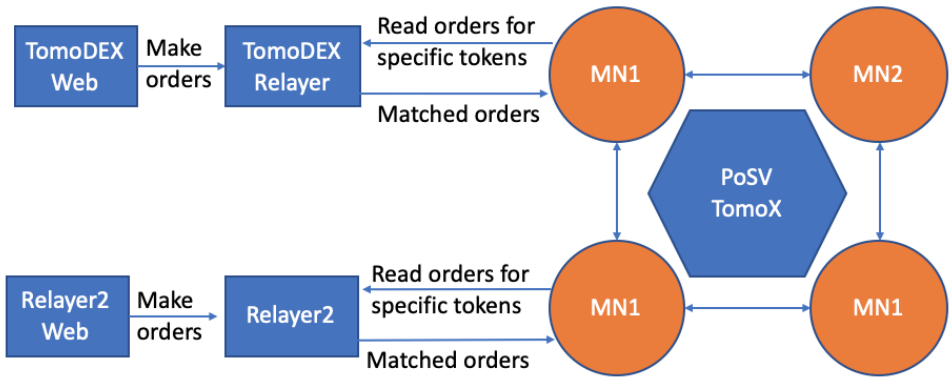
RELAYER AND MASTERNODES

As pointed out in the Section Introduction, building a decentralized exchange and operating it to provide enough liquidity are difficult in different aspects, including technicalities, marketing strategies and financial resources. TomoX Protocol addresses this problem by providing a Relayer-Masternode architecture.

Why do we need multiple relayers?

The rationale behind the Relayer-Masternode architecture is as follows - if there are thousands of tokens for trading and there is only one relayer, there are several problems:

- Thousands of traded tokens on a relayer would make the exchange user interface/experience inefficient.
- A single company would need substantial financial resources to market thousands of tokens to traders.
- Because of differences in culture and geographic regions, traders from different regions have interest in different sets of tokens, thus requiring the decentralized exchange operator to have different marketing strategies for different geographical regions.



Advantages of Relayer-Masternode architecture

Instead of having a company create both a decentralized protocol and market it, the idea of a Relayer-Masternode TomoX Protocol is to let many companies and/or decentralized business makers create their own relayers that target different sets of tokens. The relayers are responsible for providing liquidity and trading pairs for a specific set of tokens (initially TOMO/TokenX) for their target traders/users. The advantages of this Relayer-Masternode architecture are as follows:

- All relayers interact with the standardized TomoX Protocol directly integrated into the core TomoChain layer. This means relayers do not need to utilise substantial funds building the underlying decentralized exchange protocol, thus significantly reducing development as well as maintenance costs.
- All relayers can therefore focus on marketing and liquidity development.
- A relayer intended for a specific geographical region market can optimize their marketing strategy towards trading pairs that are of interest to local traders. For example, a relayer in Hong Kong or Singapore would support a different set of tokens than those of a relayer in Africa.
- A relayer can read maker orders for specific tokens from the decentralized order book of a masternode to enrich its liquidity. On the other hand, a relayer can host a matching engine and an order book for some specific tokens. The matching engine of the relayer can produce a set of matched orders from the relayer's local order book. The matched orders are then sent to the masternode's TomoX-SDK for finalizing the trade execution. Local matching engines of relayers can significantly reduce the computation load of masternodes' matching engine.

Incentives for Relayer operators

There is an incentive mechanism to encourage exchange operators to form relayers. One incentive is that masternodes do their computation for order matching and trade execution. Another incentive is that relayer operators can focus on regional marketing strategies to attract

traders and have local matching engines and order books. We believe that there should be an incentive mechanism which distributes trading fees to masternodes and relayers.

Paying trading fees by tokens

TomoX is designed to support paying trading fees by tokens. TomoX has learned the best user experience from existing CEXs. Users of TomoX will pay trading fees in tokens instead of having to hold TOMO in their wallet as in the majority of existing DEXs which have less smooth user experience than CEXs.

Trading fees flow as follows:

- Traders will pay Relayer Owners trading fees in tokens that the traders are trading in. The amount of token fees depends on each relayer, whose relayer owner can change at any time.
- The network fees that are sent to masternodes for verifying trade orders are paid by relayer owners by means of a deposit. There is a flat fee of **0.001 TOMO** per trade that a relayer must pay masternodes. The fees will go to the **Masternode owner's address.** Depending on network conditions and TOMO price, relayers can change token fees for having the best profit but also attracting traders to use their relayers.

Liquidity network

TomoX and Relayers will provide a liquidity network where all relayers share the same liquidity and trading pool. It means orders created by a relayer can be successfully traded in another relayer. In order to identify the source relayer from which a trade order is created, the trade order contains the identity of the source relayer, which is the TOMO address of the relayer owner that is registered in the TomoRelayer smart contract. This allows all masternodes to pay trading fees to proper relayer addresses.

How to become a Relayer

In order to become a relayer and receive trading fees, a relayer owner must **deposit 25,000 TOMO to the TomoRelayer smart contract.** This process is also used to transfer relayer ownership to another relayer owner.

The 25,000 TOMO deposit will be divided into 2 parts:

- **Locked Funds**: 20,000 TOMO will be locked and only be available for withdrawal 30 days after the relayer owner makes a decision to resign.
- **Trading Fee Fund**: 5,000 TOMO will be used for paying network fees, and be deducted from as fees are sent to masternodes for handling trades and order processing.

A Relayer owner can resign the relayer position at any time. If the Trading Fee Fund is not empty, the relayer owner can withdraw the remaining funds along with the locked funds **4 weeks** after resigning.

A maximum number of 150 Relayers can be launched and run. New slot availability will only be possible when an existing Relayer resigns.

Relayer Ownership market

Because the number of relayers is limited, a relayer owner can decide to sell the ownership of relayer to a buyer. This allows for a secure, decentralized exchange of relayer ownership. The procedure is as follows:

- **Relayer Owner** creates a sell broadcast through TomoRelayer website, which makes a transaction to the smart contract. The sell broadcast contains the price in TOMO that the relayer owner is willing to sell the relayer ownership at.
- **Relayer Buyer** creates a transaction by sending the exact amount of TOMO to the TomoRelayer contract in order to buy the relayer ownership and become the new owner of the relayer.
- **Once the transaction is confirmed,** the former owner of the relayer will receive the exact amount of TOMO that the buyer has sent to the contract. Any remaining amount, beyond the purchase price, is treated as part of the new owner's deposit.
- **Trading fees** will be sent to the address of the new owner of the relayer.

We believe that this Relayer-Masternode architecture will gradually build up a strong relayer-based decentralized exchange around TomoChain's masternode architecture and continue to strengthen the TomoChain ecosystem and token economy.

TOMOX PROTOCOL SUMMARY

- **Performance**: The TomoX Protocol is integrated into the core TomoChain blockchain consensus layer, which can potentially handle many thousands of transactions per second. Furthermore, with the Relayer-Masternode architecture, the heavy computational load of the matching engine for the masternodes can be substantially moved to the Relayers' local matching engines. Performance of the TomoX Protocol should be a significant improvement compared to most of the existing DEXs.
- **Liquidity**: This is a chicken and egg problem. Traders do not join most of the existing DEXs because there are not enough orders on these DEXs to match. We believe that with the Relayer-Masternode architecture and the liquidity network of relayers, each relayer can focus on understanding their relevant markets and trading pairs - thus is the potential

for better and targeted marketing strategies to attract more traders to participate in the ecosystem.

- **Full decentralization**: Most of the existing DEXs are semi-decentralized. For example, IDEX requires traders to deposit their tokens to their centralized server and all orders are stored on this centralized server. Even though the traders still have full control of their assets (because the centralized server does not know the private keys of traders), there is still a single point of failure - the centralized server. If the server is attacked, all orders can be lost. Alternatively, if the server is corrupted, it can do front-running attacks since it controls how orders are matched. TomoX Protocol, on the other hand, is fully decentralized because the order book database, matching engine and trade execution mechanism are decentralized to all masternodes. As a result of this decentralization power in TomoX, it can significantly reduce front-running risks that currently appear in some centralized exchanges and semi-decentralized exchanges.
- **Security**: As previously described, centralized exchanges have some safety and security problems. These problems have resulted in some of the biggest exchange attacks, such as MtGox and Bitfinex where 850,000 BTC in 2014 and 120,000 BTC in 2016, respectively, were stolen. These attacks happened and were successful because of a single point of failure problem in centralized exchange architecture where traders on do not have control of their private keys. TomoX and its decentralized exchanges generally solve this problem because the users have complete control of their assets. However, while some DEXs require traders to deposit their assets, TomoX does not impose this requirement on traders.
- **Cost**: TomoChain provides near-zero transaction fees, which significantly reduces trading fees compared to most existing DEXs.
- **Interoperability**: TomoX will support cross-chain exchanges so that traders can interact with and exchange other native tokens of other blockchain infrastructures - such as ETH and BTC. Atomic Swap techniques will be used for improving interoperability.
- **Accessibility**: Fiat integration has been missing in most existing DEXs. While TomoX Protocol does not directly support exchanges between fiat currencies and cryptocurrencies, Relayers have the potential to provide this service.

REFERENCES

Github repositories:

- TomoChain source code: https://github.com/tomochain/tomochain
- TomoX-SDK source code: https://github.com/tomochain/tomox-sdk