

# Bynet Protocol

[www.bynet.io](http://www.bynet.io)

[www.byron.network](http://www.byron.network)

## Abstract

Bynet Protocol is a non-custodial, decentralized set of protocols, smart contracts, codebases, and software built for Cardano Blockchain and Plutus smart contract platform designed for the extended EUTxO model introduced by Cardano. Bynet presents a new approach for on-chain order book liquidity, matching, executing transactions based on the “extended unspent transaction output” model.

## Disclaimer

The information included in this Whitepaper is subject to change or update and should not be interpreted as a commitment. Byron Network (entity behind Bynet Protocol) has the right to adjust the development process supposing the right reasons to do so appear.

<b>Abstract</b>	<b>1</b>
<b>Disclaimer</b>	<b>1</b>
<b>Introduction</b>	<b>3</b>
<b>EUTxO model on Cardano</b>	<b>4</b>
<b>Hydra, Basho era and scalability</b>	<b>5</b>
<b>Bynet Protocol</b>	<b>6</b>
Phase 1 - On-chain Order Book (Layer 1)	6
Liquidity providers	7
Liquidity Pool	9
Partially Fulfillable Order	11
Phase 2 - Matching Engine (Layer 2)	14
Matchmaker	14
Matching process	15
API - On-Chain Order Book access	16
Matching process - use case	16
BynetDEX - first dapp on Bynet Protocol	17
DEX participants	17
Advanced calls	18
Order Book Pattern	19
Liquidity Order use case	20
Bynet Wallet - mobile non-custodial wallet	21
Wallet functionality	21
<b>Cardanomarket.io - Cardano Native Tokens prices, charts, and more</b>	<b>23</b>
<b>BYNET token and its utility</b>	<b>24</b>
<b>References</b>	<b>25</b>

# 1. Introduction

Nowadays, Decentralized Finance (DeFi) trading markets use the Automated Market Maker (AMM) model created and introduced by Uniswap decentralized exchange for Ethereum and other EVM-based chains. After Cardano stepped into a new “era” called [Goguen](#), many developers (including us) started implementing multiple solutions to allow running decentralized applications for DeFi purposes [1]. It quickly became apparent that the model used by Cardano (eUTxO - extended Unspent Transaction Output) is not a proper architecture of blockchain to build clones of AMM such as Uniswap. The community quickly became aware of so-called “transaction congestions.” Using output by only one transaction at a time became a problem for the scalability of AMM-based solutions.

As Byron Network (group of developers who participated in “Plutus Partnership Program” as BinarApps before), we decided to create a decentralized exchange (initially called ByronDEX) based not on the AMM model but OBP (Order Book Pattern) model. It became evident that the eUTxO model works perfectly as a base for creating order books built out from transaction outputs as orders. The next step was to solve other challenges - how to provide liquidity, how to effectively match orders, and execute transactions staying still in a decentralized world of Cardano.

The goal of Bynet Protocol is to achieve an ecosystem that allows traders to use necessary trading tools to guarantee risk control, ease of use and user satisfaction. We aim to be the first token exchange choice layer for Cardano.

## 2. EUTxO model on Cardano

To understand the uniqueness behind Cardano and the reason why it is essential to contribute to such a thought-through project, this section will go over the most critical features of Cardano.

Known blockchains use either an account-based model, such as Ethereum, or UTxO model, such as Bitcoin. However, the team behind Cardano blockchain noticed the potential of UTxO while also implementing specific changes to ensure the great potential of their blockchain. Double spending is just one example of an issue that is not a concern for Cardano blockchain participants.

One of the changes applied by the Cardano team to the already existing UTxO was adding “datum” to transactions outputs. It is an extra argument passed in the validation process and is used to bear the state of the state machines. The second modification is “context”. Its data allows the validator to carry out more complex conditions. Cardano’s last significant change includes the validity interval to transactions, between which a given transaction will be processed.

The expertise behind Cardano mirrors the values of Byron Network and Bynet Protocol. We want to build something of use to the community. That is why the scalability, cheap fees, or achievable amount of transactions per second play a significant role in creating a trustworthy and widely used ecosystem.

Even though our products will be fully functional on Layer 1, we work with Layer 2 solutions on Cardano, which are going to revolutionize the scalability that is so important in DeFi products.

### 3. Hydra, Basho era and scalability

Cardano Blockchain development is divided into eras. As we are now experiencing working smart contracts on mainnet, scalability and interoperability is the next phase called the Basho era. This part of development is crucial for Bynet Protocol, and we aim to take part in the development of the core of the Basho era.

Whereas previous development eras focused on decentralization and new functionality such as smart contracts, Basho is about improving the network's performance with high transaction volume. This part of the development phase introduces sidechains: interoperable with the main Cardano chains. Sidechains are designed to off-load work from the main chain and increase the network's capacity. Overall, the goal is to make Cardano one of the most high-performance, resilient, and flexible blockchains.

One of the projects developed by the Cardano team is Hydra - a set of protocols designed to address network security and scalability capabilities. Hydra offers increased throughput, minimized latency, and cost-efficient solutions without substantial storage requirements. Having this part of the evolution of Cardano, our team approaches a rethought way of running an on-chain order book execution (matching and transacting) on layer 2. [\[2\]](#)

## 4. Bynet Protocol

Bynet Protocol is a non-custodial, decentralized set of protocols, smart contracts, codebases, and software built for Cardano blockchain and Plutus smart contract platform designed for extended UTxO model. Bynet introduces a new approach for on-chain order book liquidity, matching, executing transactions based on eUTxO model-based blockchains.

### 4.1. **Phase 1 - On-chain Order Book (Layer 1)**

Byron Network offers a foundation to build trading products, utilizing an infrastructure layer that enables development on the Bynet Protocol. Shared liquidity among DApps that is initiated by BynetDEX's Liquidity Providers solves the problem of lack of liquidity that any new project faces. Having mass adoption in mind, Byron Network aims to provide a development layer that is ready to implement and compose with projects like Bynet DEX. The need to build a DEX from scratch is avoided. Considering the constant-changing blockchain ecosystem's pace, projects need a foundation not to waste time on liquidity providing or market-making.

Creating an ecosystem of DApps that are intertwined with each other leads to more significant opportunities for match-making. Infrastructure that Bynet Protocol gives access to consists of initial liquidity, swapping Cardano native tokens, an off-chain match-making engine, and mobile wallet integration. Thanks to the on-chain order book pattern used in the infrastructure, trading applications can use advanced trading options like limit or stop-loss orders.

That way Bynet Protocol can contribute to the ever-growing Cardano community and provide developers with tools that help with expanding the Cardano ecosystem.

## Liquidity providers

Liquidity Pools are sets of discrete Liquidity Orders, where each order has a slightly different rate. Every Liquidity Order is an independent exchange offer, but all of them together simulate the operation of the classic Liquidity Pool. The Liquidity Provider can add their funds in particular sets of liquidity instead of through one or more Liquidity Orders with identical rates. Thus, Liquidity Pool's funds earn better in an environment of ever-changing cryptocurrency prices. Similar to AMM's concentrated liquidity pool, the Liquidity provider chooses the price range he wants to provide tokens in. They can select the range depending on the dynamics of the price of a given token. In addition, they choose how their UtxO distribution is going to form based on the formula with an adjustable function:

$$f(x) = \frac{n}{\left(\left|\frac{x}{m}\right|\right)^3 + 1}$$

Where

$n$  indicates the number of tokens in the UTxO closest to the market price (the biggest UTxO),

$m$  influences the concentration of tokens around the market price, changing the number of tokens across exchange rate values.

Liquidity Provider decides, based on the trade history, what is the dynamic of the price, and chooses the appropriate function.

- Increasing the value of  $m$  will create less concentrated liquidity,
- Decreasing the value of  $m$  will create more concentrated liquidity.

Then, they decide about the number of UTxO they want to create and the range of exchange rates. The more UTxOs, the easier it will be for matchmakers to execute orders. Therefore, more swaps equal more fees on the orders. Supposing a liquidity

provider chooses to create 5 UTxOs, the UTxOs that would be created have the following prices:

$$P_m, P_m - i, \dots, P_m - 4i,$$

Where

$i$  is a change between each consecutive exchange rate,

$P_m$  is the market price, or the price Liquidity Provider chooses according to their initial investment

The UTxOs created can be visualized by Figure 1, showing exemplary  $f(x)$  and five separate UTxOs, each with a different exchange rate, as depicted above. Creating separate UTxOs with varying exchange rates protects liquidity providers from an inadequate exchange rate to the current demand for a specific token.

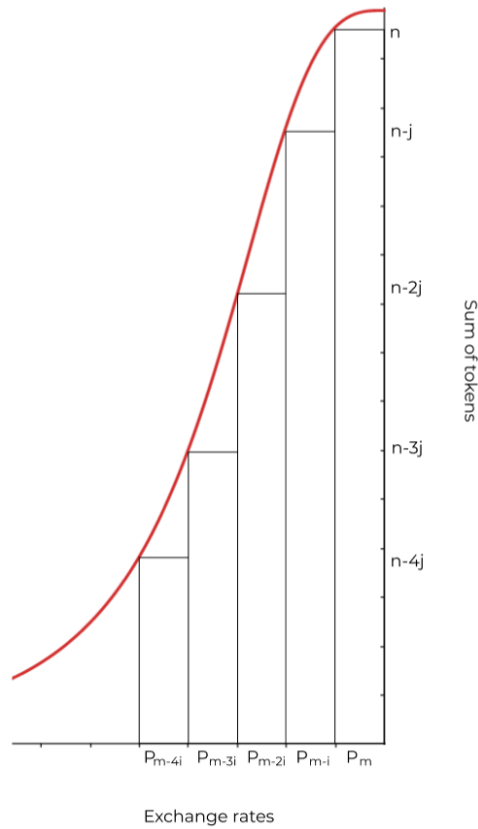


Figure 1. UTxO distribution across exchange rates



Imagine a traditional Liquidity Pool. It is a system containing large amounts of two different tokens, A and B, that allows pulling them out as long as specific rules are adhered to. For example, we can make it so each swap must additionally draw 0.3% less than it would like (a commission). If we analyze such a pool, it turns out that each consecutive swap of coin A for coin B is less and less profitable. If we were to establish that each swap could move only 100 coin A (and as much B as the algorithm of this pool requires), we could divide the entire pool into a set of independent exchange offers.

Not every offer is equally profitable - similarly to Order Book CEX, only some of the orders will be close to the market rate. However, when the global market price of coins fluctuates, the A to B swap offers will disappear faster than B to A (or vice versa). The situation will stabilize when the most profitable offer remains. As seen in Graph 1, with the demand for tokens that have been provided, the exchange rate is getting more competitive, matching the fluctuation in market price.

### **Liquidity Pool**

The liquidity pool with both tokens can be depicted in Figure 2. In this case, we look at a pair of tokens A and B as an example, where different functions have been applied. On the left side of a market price  $P_m (A/B)$ , the exchange rate would be  $P_m - i$ , meaning that A token is more expensive than a B token; a trader would want to sell A tokens. On the right side, where the exchange rate is  $P_m + i$ , the A token is cheaper than B; the trader wants to buy it. It portrays a typical situation on centralized order book exchanges. Because the Liquidity Provider imposes a fee, the actual exchange rate will be affected, and a spread would be created. Its size would depend primarily on Liquidity Provider's fee. The DEX will provide historical data to help adjust trading strategy to match trends, typical spread size in a given token pair, or the transaction sizes.

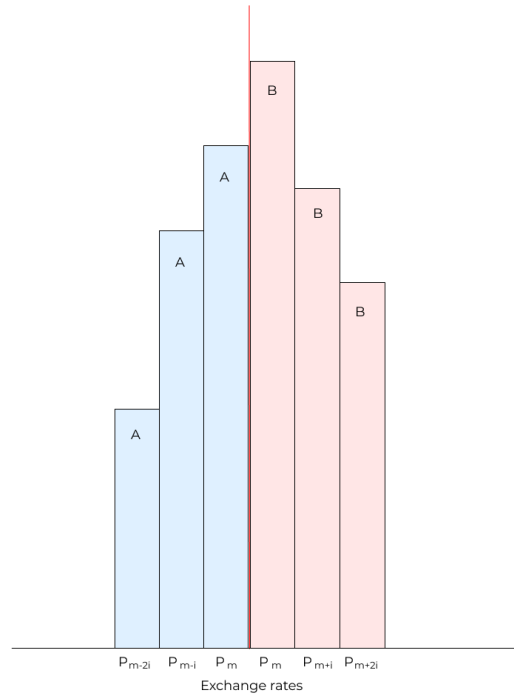
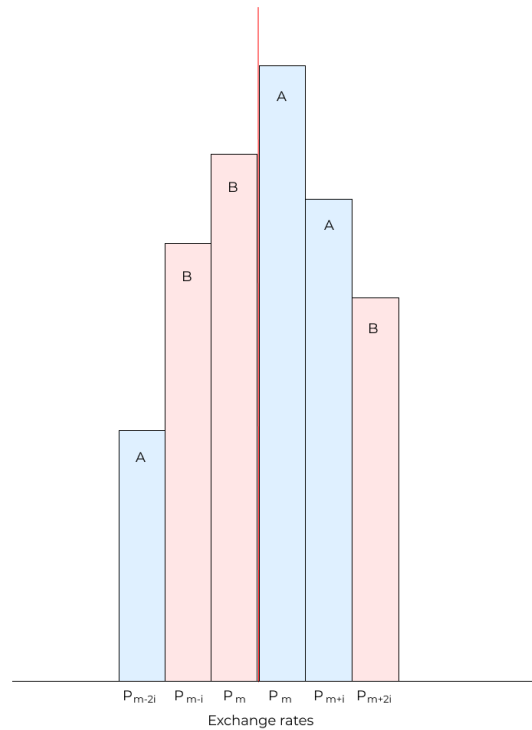


Figure 2. The initial state of a liquidity pool

Let's now suppose that several UTxOs have been swapped, a fee has been added, and now the UTxO is now selling the opposite token with the same exchange rate as previously, as seen in Figure 3.



*Figure 3. Liquidity Pool state after some swaps*

Since, for example, UTxO, which was previously selling B tokens, is now selling A tokens but with the exact exchange rate (on the right side), this UTxO is very attractive to the trader. The Liquidity Provider still imposes the fee, so he doesn't account for any losses. What is more, that kind of Liquidity Order allows for more frequent fee addition because the UTxO becomes so attractive it can be swapped immediately, increasing the Liquidity Order size. When the Liquidity Orders grow to a certain level, the Liquidity Provider can cancel them and get a number of tokens greater than the value of the initial Liquidity Order.

### **Partially Fulfillable Order**

With a market that is considered illiquid, order book needs to consider various order sizes. Partially Fulfillable Orders allow matchmakers to divide UTxOs into specified sizes, supposing requirements are met.

We define Liquidity Order as

$$\text{Order} = (A, B, \text{Fee}, R, M)$$

where:

**A** - the current amount of A tokens

**B** - the current amount of B tokens

**Fee** - the value expressed as a percentage by which each swap must be increased (e.g., 0.3% is 0.003 in this case, 50% is 0.5, etc.)

**R** - exchange rate, understood as (value of one A token) / (value of one B token)

**M** - a minimum swap size. The Liquidity Provider may not allow too small swaps if it deems that they will not bring them enough profit and will block UTxO for larger swaps simultaneously. **M** is expressed as a fraction of the range (0.1] (0.0 means that there is no lower limit for the swap size; 0.1 means that a minimum of 10% of funds must be swapped; 1.0 means that all funds must be swapped, which gives us the classic non-partially-fulfillable Liquidity Order).

### Swap A → B

On a given order **Order** = (**A**, **B**, **Fee**, **R**, **M**), you can swap **Ax** → **Bx** (we deposit **Ax** coins A and receive **Bx** coins B) when the following statements are true:

- **Bx** ≤ **B** (you cannot draw more coins than are currently available in the order)
- **Bx** / **R** ≥ (**A** + **B** / **R**) \* **M** (the value of B coins withdrawn cannot be less than the set percentage of the total value of A and B coins available)
- **Ax** ≥ (**Bx** / **R**) \* (**1** + **Fee**) (the value of the deposited A coins must be at least as much as the B + Fee coins are worth)

After such a swap, the person who created the transaction receives **Bx** coins B and creates a new order **Order** ' = (**A** + **Ax**, **B** - **Bx**, **Fee**, **R**, **M**), thus losing **Ax** coins A.

### Swap B → A

On a given order **Order** = (**A**, **B**, **Fee**, **R**, **M**) you can swap **Bx** → **Ax** (we deposit **Bx** coins B and receive **Ax** coins A) when the following statements are true:

- $Ax \leq A$  (you cannot draw more coins than are currently available in the order)
- $Ax \geq (A + B / R) * M$  (the value of A withdrawn coins may not be less than the agreed percentage of the total value of A and B coins available)
- $Bx / R \geq Ax * (1 + Fee)$  (the value of B coins deposited must be at least as much as the A + Fee coins are worth)

After such a swap, the person who created the transaction receives  $Ax$  coins A and creates a new order  $Order' = (A - Ax, B + Bx, Fee, R, M)$ , thus losing  $Bx$  coins B.

The case where  $M = 1$

If the Liquidity Provider sets  $M = 1$ , it creates a regular, not partially fulfillable liquidity order. Let's see on the example of  $A \rightarrow B$  what the formulas will look like:

$$Bx / R \geq (A + B / R) * M \Rightarrow Bx / R \geq (A + B / R) \Rightarrow (Bx - B) \geq A * R$$

We know from this equation that  $Bx \leq B$ , so  $(Bx - B) \leq 0$ . A determines the number of available A tokens in the Liquidity Order, i.e. it is a natural number - it cannot be less than zero. R as the ratio of prices A to B must be greater than 0. In this case, the inequality  $(Bx - B) \geq A * R$  is satisfied only when both sides of it are 0. A must necessarily be 0, and Bx is equal to B. In this case, we can describe the initial order as  $Order = (0, B, Fee, R, M)$ , and after replacing Ax with Bx, a new order is created  $Order' = (Ax, 0, Fee, R, M)$ .

As we can see, only one type of coin can be kept in such an order at a time, and with each swap, the entire reserve of the coin held there is converted into a new reserve of the second coin.

## 4.2. Phase 2 - Matching Engine (Layer 2)

Cardano, as its base, has three rules. Those are scalability, interoperability, and sustainability. Along with the Basho era and works around these three rules, Bynet Protocol aims to deliver Layer 2 for scalable and secure matching orders and executing transactions.

Bynet Layer 2 aims to bring scalability into transactions between orders from On-chain Order Book. We especially look at Hydra development, which can influence the speed and efficiency of transactions. Our goal is to introduce the concept of decentralized Match Making machines that take part in the whole Bynet Protocol as providers of effectiveness and efficiency.

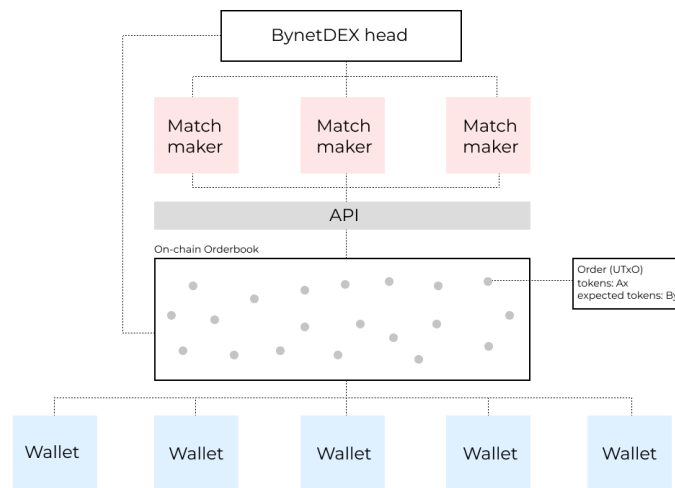


Figure 4. Matching - layer interaction

### Matchmaker

Matchmaker (aka Performer) is an SPO (Stake Pool Operator) that runs Hydra node along with BYNET Layer 2 software services.

Stake Pool Operator is a node of the Cardano P2P network that takes part in creating blocks. The more ADA is delegated to SPO, the higher the chance for SPO to become a slot leader, which means he creates a block shared in the network. There is an incentivization involved in being a block creator. These rewards are divided between SPO's operator and wallets that delegate ADA with them.

In Bynet Protocol SPOs have a crucial role. The first is making Cardano decentralized, and the second is caring about the Community. We want them to be incentivized additionally for being Bynet Protocol's Layer 2. They have the opportunity to become Matchmakers. Their role in Cardano is giving computing power to the network. This computing power may be used to keep Bynet Protocol working as well.

### **Matching process**

Matching is a service that executes transactions on Layer 2 chain. Also, Matchmaker decides how much it earns. There are two sources of transaction parameters: described by the order owner (how much they want for the tokens) and described by Bynet On-chain Order Book (mostly incentives parameters). The role of Matchmaker is to create transactions between orders and meet expectations defined in orders' parameters. It's up to the Matchmakers what reward they take. Their compensation is based on the spread between the bid and ask. Matchmaker plays on its own in a game of incentives by playing the same rules for anybody. If they want to earn more, they will focus on searching for orders that bring them a lot of rewards. But at the same time, they understand that those types of matches occur less frequently than the smaller fees ones. Matchmakers can also execute partially fulfilled swaps when the exchange rate is matched. However, there is a difference in the number of tokens that are expected.

It's a **self-balancing open market**—minimum of algorithmics, mostly open market economy. Initially, there will be one Matchmaker machine, and it will be a BynetDEX one. Once this model is confirmed, the Community will get access to the code (software) to create their machines and participate in the “matching game”. We will

support SPOs Community to join the protocol as Matchmakers on specified markets. SPOs as separate instances of the DEX working on On-chain Order Book from Bynet [3].

### API - On-Chain Order Book access

In our protocol, we introduce API endpoints to be accessible by Matchmakers. Thanks to this layer, Matchmakers can easily ask for data from On-chain Order Book. Data response (JSON) consists of a list of orders and order details. Requests are parametrized, meaning Matchmaker can decide what type of orders they want to get, how many of them, how sorted and ordered, etc. It is similar to database queries.

```
[
  {
    "lockedCoin": {
      "amount": 1000,
      "coin": {
        "currencySymbol": "25ae866bd6b617664c054dc97f4d5b3a8cff3fb6ab0354622ada4a11",
        "tokenName": "A"
      }
    },
    "orderType": "Liquidity",
    "orderHash": {
      "txOutRefIdx": 1,
      "txOutRefId": {
        "getTxId": "9dec4e3d5cd0b7c1265bdd4e8642d95ec3465e309427cb7288c946d25d09fc7d"
      }
    },
    "expectedCoin": {
      "amount": 100,
      "coin": {
        "currencySymbol": "25ae866bd6b617664c054dc97f4d5b3a8cff3fb6ab0354622ada4a11",
        "tokenName": "B"
      }
    }
  },
]
```

Figure 5. Example of JSON response

### Matching process - use case

Matchmaker focuses on one pair of tokens: Token A and Token B. They see that the current exchange rate between them is 1A:2B. Its goal is to find the best orders to bring them at least, e.g., 0,3 ADA. They have to look into the On-Chain Order Book, limit



orders to those in this pair, find the opposite ones and then try to match them with the minimum of 0,3 ADA worth of tokens as a reward left for themselves. This takes some time, and there might not be any order meeting those expectations at all. It's also a risk for them because while searching is more prolonged, another Matchmaker can already use UTxOs that meet his expectations. The matchmaker then reconsiders its plan. It's worth finding those who are leaving 0,05 ADA because based on the analysis of OOB, there will be more earnings in total, as those are faster to find at the current price.

### 4.3. BynetDEX - first dapp on Bynet Protocol

Decentralized apps, in particular decentralized exchanges, have been getting more and more attention with the possibilities they offer. Without the need for a third party, DEXes offer their participants a wide range of incentives. BynetDEX allows the exchange of native Cardano crypto assets between the users. The development and introduction of multi-chain will welcome swaps with any crypto assets, regardless of their blockchain.

Apart from being traders, participants of the DEX will be given a choice to become a Liquidity Provider or a Matchmaker. Having various economic incentives, one can decide which role fits their strategy best. In addition, Bynet DEX users are going to be able to use the wallet of their choice, whether that would be Bynet Wallet prepared specifically for Bynet DEX or any other integrated Cardano wallet.

#### **DEX participants**

We have 3 types of actors:

**traders** - those are the traders interested in exchanging their crypto assets for other crypto assets without the intervention of any third parties. Traders' objective is to swap the assets with the most optimal price possible. They will be able to use trading options such as limit order or stop-loss order. The trading experience will be close to what

traders find familiar with CEX. In addition, these types of orders are thought to be a fundamental part when discussing risk management.

Traders have to have in mind that orders that are supposed to be swapped as soon as possible need to have an exchange rate that is a little less attractive to them, or they should create an order with additional ADA as an incentive for matchmakers. The swap order that the trader creates is more attractive for a matchmaker as it covers the cost of making a swap.

**liquidity providers** - people with funds willing to provide liquidity. Liquidity providers earn from fees that are given upon their liquidity orders. The liquidity providers choose fees. They are given freedom regarding the amount of fee they decide to put on a particular liquidity order. That way, they are incentivized to manage their risk strategy. In addition, they can preview their rewards and withdraw them while contributing to the DEX by sharing a percentage of their profit.

**matchmakers** - people (or bots) executing orders. They look for orders that match and choose the ones from which they can earn. For example, Alice wants to trade 10A for 9B, and Bob wants to trade 10B for 9A. Both of them want their orders to be executed as fast as possible. Therefore they choose a less attractive exchange rate. If we take these two orders and execute them in one transaction, Alice gets 9B, Bob gets 9A, and the performer gets 1A and 1B. Performers want to be able to easily analyze existing DEX orders and combine as many orders as possible into one transaction. Matchmaker has to stake a required amount of BYNET tokens to execute matches. In the initial stage of BynetDEX development, the role of matchmakers will be given to SPOs.

### **Advanced calls**

ByronDex distinguishes two modes in which a user can trade. The first one is a simple swap-mode, similar to Uniswap style, with the option to choose slippage. The second one is more complex as it combines several types of orders. We call the second type an

**orderbook-mode.** It comprises orders such as market limit order, stop-limit order, stop-loss order, stop market order, trailing stop order.

## Order Book Pattern

The Bynet DEX model is based on Order Book Pattern (OBP) combined with a 2-phase commit pattern. The model distinguishes the commit and execution phases. In the committing phase, swappers submit crypto asset orders to expect a particular amount of an opposite coin. The execution phase matches orders and performs them accordingly. Successful execution locks money in the script for the beneficiary. Like CEX, the UI will include a list of buy and sell orders, and with progress, the charts with market depth will visualize the current market situation.

Orders are the core of OBP. Order is represented as EUTxO, which contains all information needed to perform a swap. There are different types of orders making up the model. In the first version, we implemented the following:

**Swap order** - a type of order that applies market order features. Traders give it out with all the necessary information. It contains the tokens that the trader wants to replace, and they can be used only when an appropriate payout is created for the owner of the order (UTxO, which that person can only use). Swap order is simple UTxO pushed into On-chain Order Book and expected to be executed as fast as possible by Matchmaker with the opposite swap order. After the swap is done, new UTxOs are created and assigned to the owners with a number of expected tokens.

Traders can use advanced trading options with order types like limit order or stop-loss order. That way, they are given more control over their long-term investment, allowing them to wait for a specific exchange rate.

**Liquidity order** - a type of order prepared with liquidity providers in mind. It contains information about which two tokens (in specific quantities) will be exchanged

and the amount of the fee. The fee that the liquidity provider imposes is not specified; rather, we want traders to apply a particular fee considering their risk strategy. The formula that explains the behavior of a liquidity order after being swapped in terms of one specific token can be described as follows:

$$T_n = T_0(1 + f)^n$$

where

$n = 0, 2, 4, \dots$ ,

$f$  is a fee imposed on the order by liquidity provider,

$T$  is the number of tokens in a liquidity order

### **Liquidity Order use case**

A trader manually creates a liquidity order between 100A and 50B, with a commission of 1%. In the beginning, we create it as UTxO and add 50B to it. If someone wants to receive 50B, they will have to create a new liquidity order with at least 101A (101% of 100). Now the liquidity order has 101A and awaits at least 51.005B (101% of 50.5, which is a calculated amount for a given exchange rate), meaning that if someone wants to get 101A, they will have put at least 51.005B in it. This works until the original owner cancels the order - then they receive all the funds stored in this UTxO. The more swaps are made on this liquidity order, the more profit the person submitting it will receive.

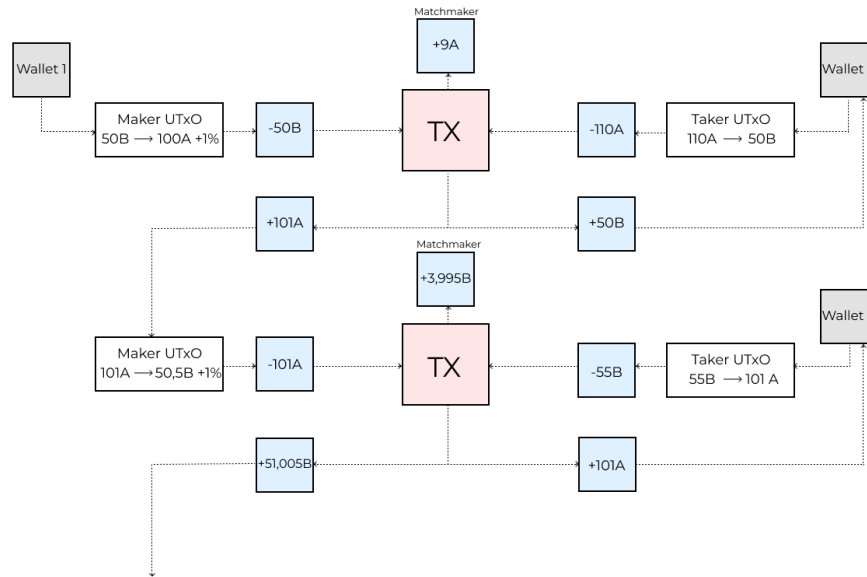


Figure 6. Liquidity Order use case

#### 4.4. Bynet Wallet - mobile non-custodial wallet

The first milestone of Bynet Protocol's tools is an HD Mobile Wallet for Cardano launched on the Google Store and Apple Store. Bynet Wallet aims to be the first choice for mobile users willing to interact with Cardano Blockchain.

Bynet Wallet is an HD Native Wallet for Cardano, part of the Bynet Protocol ecosystem. As the first of its kind on the Cardano blockchain, we plan to deliver the best quality wallet and contribute to the community by developing mobile tools useful to developing mobile DApps on this particular blockchain.

#### Wallet functionality

The functionality of Bynet Wallet includes sending and receiving crypto assets on the given wallet address with mobile security. Due to the traders-for-traders approach, the Wallet will be equipped with crypto portfolio management. Integration with Bynet DEX will guarantee trading opportunities directly from the Wallet, taking the next step

into better usability. Clear and intuitive design based on traders' experience makes the DApp user-friendly.

We understand that security plays a significant role when the topic of storing cryptocurrency arises. Specific solutions require different approaches to ciphering data, so our team considered both the market expectations and technical possibilities. Bynet Wallet guarantees multi-level security and features such as biometrics and PIN. To ensure a high-security level, we use cutting edge versions of core and encrypting libraries to provide bugless, and for more free from vulnerabilities issues place for money, such as:

- entropy storage
- entropy encrypting
- mnemonics
- signing transactions
- CBOR parsing

Process of wallet creation concerning security:

1. Entropy is generated. Public and private keys, as well as wallet addresses, are generated from entropy.
2. Entropy is encrypted using asymmetric cryptography.
3. Using react-native-keychain, the entropy that was asymmetrically encrypted is secured using biometrics on hardware, on the operating system level.
4. As the crucial element of the wallet, entropy can be used only when the user is signing a transaction. However, we send a request to the service layer to have the transaction signed to avoid unnecessary access to entropy (decrypting it).

#### 4.5. Cardanomarket.io - Cardano Native Tokens prices, charts, and more

Cardano ecosystem has grown to one of the biggest in terms of Community, TVL, Smart Contracts, and DApps number. With the number of projects, which is still growing, the number of new tokens on the market is constantly increasing.

Cardano Market is an oracle and price aggregator that displays current price estimations based on results from different decentralized exchanges on Cardano Blockchain. The price indicated on the Cardano Market is an average from data extracted from SundaeSwap, MuesliSwap, and MinSwap that is updated every few minutes. The goal of Oracle is to portray the current market situation with consideration of various price sources in an accessible form for traders. Cardano Market is available for the Cardano community both on Bynet Wallet and on [cardanomarket.io](https://cardanomarket.io)

## 5. BYNET token and its utility

BYNET token will provide incentivization on the Bynet Protocol, with 60% of the tokens being distributed to the community that actively uses the platform, adds liquidity, or stakes BYNET tokens. In addition, BYNET tokens will grant voting power to holders regarding changing protocol parameters. BYNET token is a gateway for advanced trading options, e.g., limit orders and stop-loss orders.

### **Liquidity Provider** (market)

- Liquidity Provider earns BYNETs from Liquidity Mining Program as rewards for providing liquidity.

### **Matchmaker** (computing power)

- SPO has to have a specified amount of BYNETs staked to be a Matchmaker.
- Matchmakers may share earnings with delegators - they decide what percentage of earnings from matching go to delegators (only to those delegators who stake BYNETs and reward only in BYNETs).

### **Trader** (market)

- Advanced trading options, once introduced, will have small additional BYNET fees.

### **Staker** (BYNET power)

- Earns BYNETs per epoch when keeping tokens during full epoch from “Staking” rewards treasury.

### **DAO** (Utility)

- Each owner of BYNETs has its vote power during parameters changes voting.
- BYNETs might be considered to be burdened when needed.



## 6. References

### Work Cited

- [1] Ladopoulos, Dmitris. “Goguen - Cardano Roadmap.” *Cardano Roadmap*,  
<https://roadmap.cardano.org/en/goguen/>. Accessed 6 March 2022.
- [2] Ladopoulos, Dmitris. “Basho - Cardano Roadmap.” *Cardano Roadmap*,  
<https://roadmap.cardano.org/en/basho/>. Accessed 6 March 2022.
- [3] “Implementing Hydra Heads: the first step towards the full Hydra vision.” *IOHK*, 2  
February 2022,  
<https://iohk.io/en/blog/posts/2022/02/03/implementing-hydra-heads-the-first-step-towards-the-full-hydra-vision/>. Accessed 7 March 2022.