



## **A Decentralized Exchange (DEX)**

That is driven by the Automated Market Maker (AMM) protocol, with the aim to provide liquidity to Cardano Blockchain projects that issue native tokens.

# TABLE OF CONTENTS

Abstract .....	3
Introduction.....	4
Why DOEX is on Cardano blockchain?.....	6
Cardano vs Ethereum .....	7
ADA-ERC20 token bridge.....	9
Automated Market Maker (AMM).....	10
Decentralized Exchange.....	12
How Cardano Projects are Overcoming the Concurrency Issue .....	12
Market analysis (DeFi).....	14
Tokenomics .....	15
Features .....	16
Utility of the Token.....	17
Roadmap .....	18
Disclaimer .....	19

# ABSTRACT

Decentralized Exchanges or DEX perform the same function as their centralized counterparts. However, with DEX, users only interact with self-enforcing smart contracts to carry out secure and non-custodial transactions without the need of centralized third parties.

This document introduces and describes DOEX – a Cardano Blockchain-based decentralized exchange that uses Automatic Market Making protocols to execute transactions. DOEX striking features include multiple pricing functions for a single liquidity pool, trade routing, instant price feed via on-chain price oracle, and automatic babel fees redemption for Stake Pool Operations (SPOs) that are Cardano Blockchain-based.

# INTRODUCTION

Although one of the top performing blockchain networks, Cardano is yet to have a native Decentralized Exchange like those seen in other blockchain networks. This means that there is no exchange list for tokens of projects that are based on Cardano Blockchain. Interestingly, this will soon become a thing of the past as DOEX is set to be the first Cardano Blockchain-based DEX with which liquidity will be provided to native assets on its network. The Cardano Blockchain update referred to as Mary Hard Fork that was completed on the 1st of March allows anyone to create native cryptocurrency assets on the blockchain. As such, it allows Cardano to have multi asset support and users can create custom tokens as well as execute transactions directly on the Cardano blockchain.

With Mary Hard Fork, Cardano blockchain now offers several tokenization options and supports the blockchain to provide transactions that involve several asset types at the same time. Native support of tokens is an important leverage for developers as it saves them the stress of using smart contracts to create custom assets or transactions. With this, the transfer of asset ownership is tracked by the accounting ledger thus removing the complexity, errors and security vulnerabilities from the equation in a cost-efficient manner. More precisely, native tokens on the Cardano Blockchain do not require the extra efforts that come with the creation of smart contracts to transfer their value and users can carry out transactions and burn their tokens without incurring smart contract transaction fees or adding event-handling logic to track transactions.

This update enables the creation of fungible and non-fungible tokens, which in turn enables users to create custom payment asset, stable coins pegged to fiat currencies, assets to represent intellectual property (IP), etc. These assets can then be used to seamlessly carry out transactions. There are three ways by which assets can be created on the Cardano Blockchain. **They include:**

- Cardano Command Line interface (CLI);
- Token Builder graphical user interface (GUI);
- Daedalus wallet.

**The lifecycle of the native assets is made up of 5 phases:**

- Minting;
- Issuance;
- Using;
- Redeeming;
- Burning.

The use of Cardano Command Line Interface (CLI) involves the technical know-how of setting up and operating the Cardano node as well as having the knowledge of handling transactions and managing wallet addresses and technical values. The GUI token builder on its own makes token creation and deployment seamless and facilitates token creation for Decentralized Applications (DApps) other specialized forms of tokens like NFTs, and fiat-pegged stablecoins. Daedalus and Yoroi wallets allow users to make use of existing assets for payments and purchases or exchanges.

DApps can be created on Cardano by taking advantage of the features brought by Goguen era developments like Mary hard fork, Plutus and Marlowe - all of which are significant developments in the capabilities of Cardano. More specifically, Plutus is a smart contract language and execution platform that consists of On-chain (on Cardano Blockchain) and Off-chain (on the user's machine) branches and uses the Haskell programming language. It allows the use of Alonzo update - as depicted in the final phase of Goguen on the roadmap of Cardano. Goguen will also deliver other core offering improvements, most importantly - multi-asset ledgers.

The Alonzo update or hardfork brings about new and promising features to the Cardano Blockchain as it will enable smart contracts on the network via the integration of Plutus scripts. Alonzo adds a lot of opportunities for businesses and developers by facilitating the development of Decentralized Finance (DeFi) focused DApps and smart contracts. Alonzo brings a systematic approach that is based on verification and formal methods to extend the simple multi-signature scripting language used in Cardano Shelley. Being an updated and extended effort on the Plutus smart contract language, Multisig ensures more efficient and stable scripting options.

Powerful scripting is facilitated by Alonzo via the use of an extended model of unspent transaction output (eUTXO). This is made possible by using the hard fork combiner technology of IOHK - the parent infrastructure research and engineering company overseeing Cardano. This leads to efficient smart contracts that facilitate seamless and efficient automated assets trading applications and large cash movements. Apart from this, developers are equipped with tools to experiment, validate, and customize Cardano transactions. The APIs library will be expanded so that it can allow the deployment and operations of Plutus Core code while communicating with wallets and the distributed ledger.

Daedalus update is the precursor of the Alonzo update, and it allows users to use their wallet to receive both ADA and several other assets on the Cardano network. The advent of Daedalus brings about the switch from platform's stake pools to community-led stake pool operators.

# WHY DOEX IS ON CARDANO BLOCKCHAIN?

Like other blockchains, Cardano has several advantages. It is scalable, fast, has low transaction fees that can be paid with the same token sent. Although blockchains like Ethereum have a higher degree of acceptance than Cardano, we trust in the Cardano Blockchain potential to attract developers and new venture capitalists which will catapult its adoption in the near future.

In addition, Cardano has a layered blockchain architecture that is composed of two main elements, the Cardano Settlement Layer (CSL) and Cardano Computational Layer (CCL), which makes it truly unique.

Most of the other existing blockchain platforms only have a single layer, which leads to scalability issues and often causes network congestion, slows down transactions and leads to higher network fees. Ethereum processes approximately 15 transactions per second (TPS). This small amount of TPS makes the network slow and congested within a short time. Cardano on the other hand does not have these scalability issues. Simulations have shown that each "Hydra head" of the Cardano network can currently process about 1,000 transactions per second. This can be combined with 1,000 stacking pools, each of which processes 1,000 TPS. As such Cardano could achieve up to 1 million transactions per second which makes it super-fast at executing transactions at a very low network fee.

Cardano and Ethereum networks have very similar properties. This includes ease of creation of smart contracts and building decentralized applications (DApps). However, the philosophical notions of their creation and their design viewpoints are quite different.

# CARDANO VS ETHEREUM



<b>FOUNDED</b>	September 27th, 2017	December, 2013
<b>CREATORS</b>	Technologists Charles Hoskinson and Jeremy Wood.	Vitalik Buterin, Anthony Di, Charles Hoskinson, Mihai Alisie & Amir Chetrit.
<b>TICKER</b>	ADA	ETH
<b>VISION</b>	<p>The primary function of Cardano is to facilitate operations in its native token - ADA and to empower the developer community to build secure decentralized applications with amazing use cases.</p> <p>Cardano emphasizes an approach that is purely based on research with the aim to facilitate mainstream adoption of the technology.</p> <p>Cardano uses mathematically verified codes to provide users and developer community with excellent optimizations that are grounded in scientific research.</p>	<p>The aim of Ethereum aimed is to become a global, open-source platform for the creation of custom assets and various DApps.</p> <p>Ethereum uses the offers several other decentralized products and use cases apart from finance</p> <p>Ethereum was adopted by various blockchain projects during the ICO rush to raise funds for their project.</p> <p>The currently most popular use of Ethereum is the creation of Decentralized Finance applications. Which is aimed at decentralizing core traditional financial use cases like lending/borrowing and removing centralized third parties and middlemen such as banks or mainstream financial institutions from transactions.</p>
<b>LAUNCH &amp; ISSUANCE</b>	<p>The Cardano Network is managed and supervised by three institutions. They include:</p> <ol style="list-style-type: none"><li>1. Cardano Foundation: responsible for the management of all aspects of the network's blockchain.</li><li>2. IOHK: created and designed the blockchain and its proof-of-stake algorithm.</li></ol>	<p>The objective of Ethereum is to be a global launchpad blockchain project where everyone can launch and run an application.</p> <p>To pursue this objective, Ethereum sold 72 million Ether (ETH). It's native currency.</p> <p>Ethereum network has a brilliant community of developers, who actively</p>

3. Emurgo promotes the adoption and industry-wide acceptance of the network's technology for various institutions.

Worthy to mention is that about 31 billion ADA tokens were created.

engage in network expansion, growth and the creation of other networks and innovative projects.

Some of them include: Gavin Wood, Jeff Wilke, Joseph Lubin, and Charles Hoskinson. They have industry experience and are now leaders in the blockchain community.

## NETWORK DESIGN

To make the network secure, Cardano uses a Proof-of-Stake-like consensus mechanism named Ouroboros. With it, users earn newly minted ADA when they validate transactions.

Time is divided into epochs and slots by Ouroboros and the epochs are wide time frames while slots are 20-second increments within the epochs.

For each slot, a leader is selected and he is responsible for selecting the blocks that are added to the blockchain.

At the end of an epoch, the previously selected slot leaders will choose the leader of the next epoch among themselves.

Smart contracts are written by developers for the creation of DApps. These smart contracts are then deployed to the Ethereum Blockchain. The Dapps can be activated once a specific goal or result is achieved.

Ethereum uses the Proof-of-work consensus mechanism to run its blockchain just like Bitcoin Blockchain. However, it will soon move to Ethereum 2.0 that runs a Proof-of-Stake consensus mechanism.

With Ethereum 2.0, any user with at least 32 ETH will be able to lock up the funds in a contract and be incentivized for solving computations that help to add new blocks to the blockchain.

## MONETARY POLICY

ADA is the native currency that drives Cardano and it is minted on every block. It is also the means by which slot leaders are rewarded for transaction verifications.

ADA has a limited supply. This means that its total supply is capped at 45 billion.

As at January 2021, 31 billion ADA were in circulation and the 14 billion tokens that are left will be issued via minting.

Like ADA, Ether (ETH) is the native currency that drives the Ethereum network. It is minted in every block and given out as reward to miners for their computing power.

There is a sharp contrast between ETH and ADA here because ETH does not have a limited supply. Rather, its supply is programmed to increase by 4.5% annually.

Changes to the monetary policies of Ethereum have been suggested by developers and it was voted upon by nodes and miners.

Gas or network fee is another core feature that drives the Ethereum blockchain. It is a unique computational unit that is applied for the computation fees.

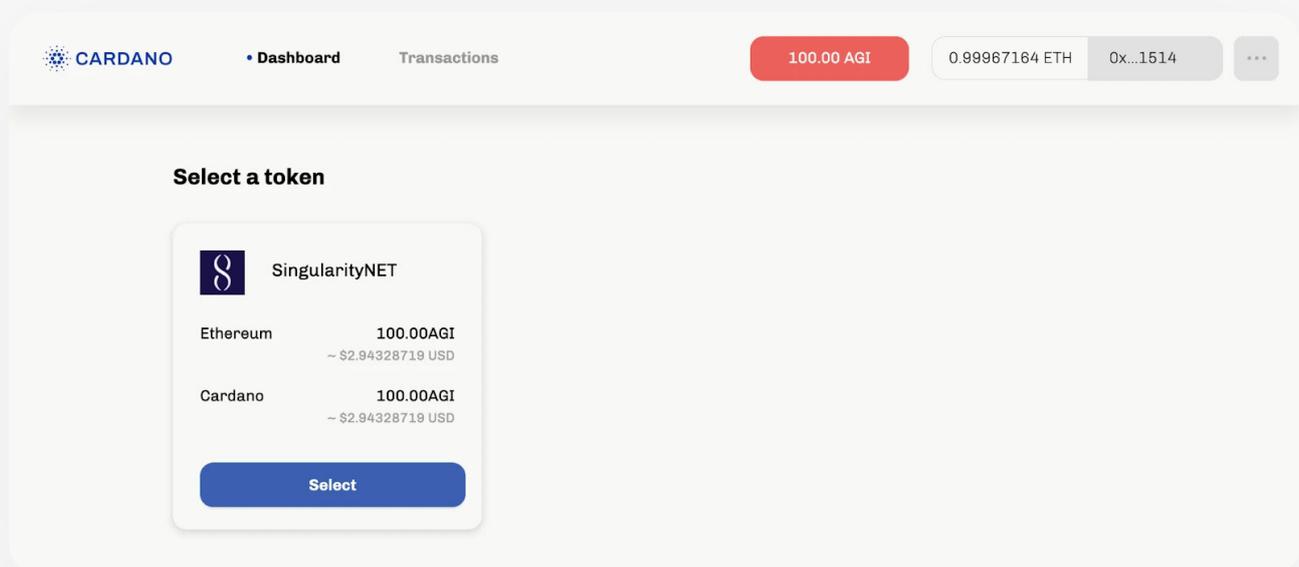
# ADA-ERC20 TOKEN BRIDGE

As earlier mentioned, the Cardano network supports ADA - its native token and the tokens of other successful projects created on its network with over 160,000 tokens minted. To ensure better interoperability across chains so that a solid background can be laid for extended business and expansion opportunities, an ERC20 converter is a sure deal.

The converter allows issuing organizations, projects and their users to handle the migration of ERC20 tokens to Cardano, i.e. it enables them to move their ERC20 based tokens to the Cardano network with just a few clicks. The converted token will have the same value and will work the same way as the ERC20 it is converted from in addition to this, users that wish to do this later can also move their tokens back to the source network by burning them on Cardano. The ERC20 converter has a 2-way convertibility baked in.

*It is worthy to mention that it is possible to use Metamask (a Chrome browser extension) to validate an account with more options to be added later. For users to be able to easily migrate their tokens to Cardano and track transactions and balances, they must add their Daedalus testnet address.*

When a user accesses his ERC20 converter account, he will see SingularityNET tokens listed and available for migration once he clicks a token. All that is required of the user to carry out a conversion is to select the token, type the amount he would like to convert and add a Cardano address to migrate the token. Once the token migration to the Daedalus wallet address is carried out, it can then be used for any payment or transaction that the user desires while the activities will be visible within both - Etherscan and the Cardano Explorer.



The screenshot shows a web interface for the SingularityNET ERC20 converter. At the top, there is a navigation bar with the CARDANO logo, a 'Dashboard' link, and a 'Transactions' link. On the right side of the navigation bar, there are three buttons: a red button labeled '100.00 AGI', a white button labeled '0.99967164 ETH', and a grey button labeled '0x...1514'. Below the navigation bar, the main content area is titled 'Select a token'. It features a card for SingularityNET with a blue 'S' logo. The card displays two options: 'Ethereum' with '100.00AGI' and '~\$2.94328719 USD', and 'Cardano' with '100.00AGI' and '~\$2.94328719 USD'. A blue 'Select' button is positioned at the bottom of the card.

The ERC20 converter will be made available for the public after the quality assurance testing is complete. At the moment, it is being tested to ensure a top-notch user experience as well as fix any issues or vulnerabilities that may exist. Relevant documentation and instructions on how the users can test the converter capabilities will soon be provided to the dedicated testnet environment.

## AUTOMATED MARKET MAKER (AMM)

AMM or Automated Market Maker exchange models are changing the narrative in both traditional and decentralized finance. It is the underlying protocol that drives decentralized exchanges (DEXs) and it is designed to exchange one token for another directly, bypassing trading platforms and other intermediaries.

Before AMM came into prominence, exchanges used to use a classical order book mechanism to match trading orders. As such, they only serve as intermediaries - matching buyers to sellers and taking a cut of the transaction. Unfortunately, they suffered from liquidity issues, caused by a number of factors, including as time required to place each order, block confirmation times and slippage issues. As a result of this, the price of an asset at the point of executing a trade can shift considerably before the trade is completed. This often occurs in volatile environments like the crypto market. Hence, the exchanges must ensure that transactions are executed instantaneously to reduce price slippages.

### How Does an AMM Work?

Automated market markers replace the conventional matching system and order books with autonomous protocols that are powered by blockchain-based smart contracts. These smart contracts define the price of a cryptocurrency asset and are also responsible for liquidity provision. As such, traders trade against the liquidity locked in the smart contract and not the counterparties like their traditional finance counterparts. Also, to carry out exchange operations using AMMs, the user doesn't need to create an account on the exchange, go through any KYC procedures or entrust their funds to third parties. All the user needs to do is connect the browser wallet, select the exchange direction, and make the transaction.

What happens next is that the smart contract will automatically send the corresponding amount of cryptocurrency assets to the user's wallet. DOEX uses this exact same method to execute the trades. The platform solves performance restrictions of AMMs that come before it by leveraging the interoperable, fast, and secure, liquidity provision features of smart contracts created on the Cardano network. A couple of points to note:

- Trading pairs exist as individual liquidity pools (LP) in the AMMs;
- Instead of using dedicated market makers, anyone can provide liquidity to these pools by depositing both assets represented in the pool.

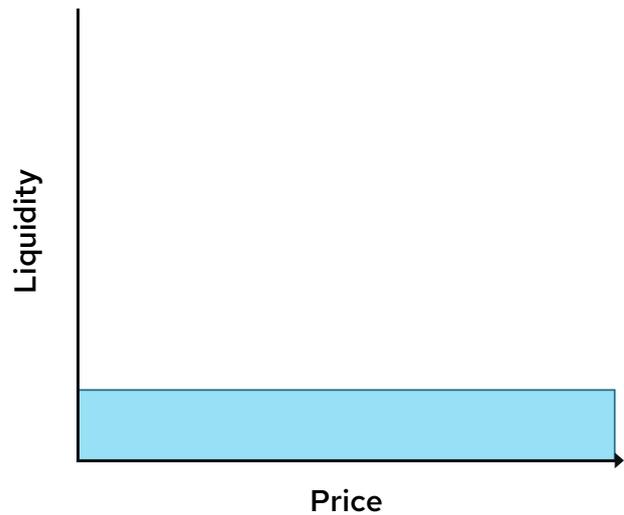
To ensure the ratio of assets in the liquidity pool is balanced, AMMs use mathematical equations and existing protocols use an equation as simple as  $X \times Y = K$  where X and Y represent the value assets A and B respectively and K is a constant.

Essentially, the liquidity pools on AMMs always maintain a state whereby the multiplication of the price of Asset A and the price of B always equals the same number.

### How AMM Liquidity Providers Earn

As earlier mentioned, AMMs use liquidity to execute trades. Whenever liquidity is deposited into a pool, special tokens known as liquidity tokens are minted to the provider's address in proportion to how much liquidity they contributed to the pool. These tokens are a representation of a liquidity provider's contribution to a pool. Whenever a trade occurs, the fee which is levied is distributed pro-rata to all liquidity providers in the pool at the moment of the trade.

To put it simply, when a user supplies an asset – provides liquidity to the pool, it automatically becomes a fungible resource. The token deposited in the liquidity pool is denoted with a value of a derivative. This gives the supplier the ownership rights of the reward paid on the total amount supplied. The assigned derivative is, thus, defined as an increasing percentage ownership claim of a portion of the liquidity pool supplied to the smart contract. With that, liquidity providers can then choose to sell, transfer, or otherwise use their liquidity tokens in any way they see fit. To summarize, when you make a deposit of your token into Liquidity Pools, you will receive an LP token and a share of the transaction fee.



*CFMMs provide liquidity across the entire price range.*

# DECENTRALIZED EXCHANGE

A Decentralized Exchange or DEX (DEX) is a blockchain-based application that is accessible through a series of smart contracts and is designed to facilitate financial services that are traditionally carried out by a central entity in a decentralized manner.

With DEX, trustless parties can carry out financial transactions by relying only on the self-enforcing ability of smart contracts. Apart from decentralizing access to financial services, it also ensures that profit from the financial services are decentralized.

Participants that provide liquidity to facilitate exchange, swap and other types of operations on decentralized exchanges are rewarded with a small fee and it serves as a means of passive income generation for individuals. Something that is only reserved for large institutions in the traditional finance.

There are a lot of existing DEXs on different blockchains. Examples include PancakeSwap on Binance Smart Chain (BSC) as well as UniSwap and Curve on Ethereum Blockchain. DOEX on its own is being built for Cardano Blockchain to facilitate the swap of Cardano Blockchain-based assets.

## HOW CARDANO PROJECTS ARE OVERCOMING THE CONCURRENCY ISSUE

### Understanding Concurrency

In general, concurrency is the ability of multiple agents to interact with the same smart contract at the same time with the intention to achieve the same result. In decentralized finance or DeFi parlance, it is the ability of a DEX to allow multiple executions of swap or exchange operations at the same time without issues. In fact, after Cardano announced the launch of the Plutus smart contract functionality on testnet, some DEXs have launched on the testnet and ran into severe concurrency issues with their DApp. Thus, being able to handle only one transaction per block, raising concerns about Cardano's capability to run smart contracts.

### Cause of the Issue

It has been observed that the concurrency issue is due to how the Cardano blockchain is using unspent transaction outputs or UTXO-accounting models rather than an accounts-based model,

used by the likes of Ethereum. As such, designing a DEX that overcomes concurrency has been tricky. Ethereum, Solana, and most other smart contract enabled-blockchains employ an account-based model to compute transactions while Cardano employs a novel iteration of Bitcoin's UTXO model called Extended UTXO (EUTXO).

The EUTXO model poses challenges for Cardano dApp builders. Account-based models allow multiple users to interact with the same smart contracts by default. However, EUTXO-based smart contract blockchains pose difficulties for developers to mitigate concurrency without making compromises on security or decentralization. From a technical point of view, the Cardano team explained in a long-form blog post that transaction validation is divided into two phases and the reason is that it should limit the amount of uncompensated validation work by nodes.

Each phase serves a purpose in achieving this goal. The first phase checks whether the transaction is constructed correctly and is able to pay its processing fee. The second phase runs the scripts included in the transaction. If the transaction is phase-1 valid, phase-2 scripts run. If phase-1 fails, no scripts run, and the transaction is immediately discarded.

### **How Projects are Overcoming the Concurrency Challenge**

Interestingly, some projects have come up with working solutions for the Cardano concurrency issue. Some of these include building DApps that tolerate segmentations of state or aggregating multiple interactions to settle on the same state. For decentralized exchanges, this would mean either fragmenting liquidity into multiple pools (states) or using third-party sequencers to batch multiple transactions and settle them as one transaction in the same state.

Other proposed solutions for scaling DApps on Cardano involve implementing Layer 2 protocols and sidechains, which deal with their own unique centralization and security challenges (while such solutions are yet to go live on Cardano, at least one EVM-compatible sidechain is in the pipeline). Also, Cardano partners are already developing solutions that can lay an account-based model atop a UTXO-type chain for developers who prefer that way of working.

# MARKET ANALYSIS (DEFI)

The DeFi niche of the decentralized finance industry is a huge niche that is set to bring core traditional finance use cases like exchange, swap, staking, lending/borrowing, currency issuance, peer-to-peer payment and even insurance on the blockchain. As a result, centralized third parties and intermediaries are eliminated from transaction activities and all of which are carried out on the blockchain.

According to DeFiPulse, the total value locked (TVL) in DeFi protocols followed an exponential trend and rose to \$87 billion in May 2021. The biggest share of the DeFi market is taken by Decentralized Exchange projects as well as infrastructure service providers such as liquidity pools or staking providers that help users to execute validation nodes for Decentralized protocols.

Decentralized exchanges executed transactions worth over \$60 billion, which is an upward trend that overshadowed the \$26 billion that was recorded in September 2020. Pancakeswap and Uniswap dominated the market in this niche and it confirms that there are still a lot of untapped opportunities in the industry especially for a project like DOEX that will be launched on a formidable blockchain network like Cardano.

## Total Value Locked (USD) in DeFi

[TVL\(USD\)](#) | [ETH](#) | [BTC](#)

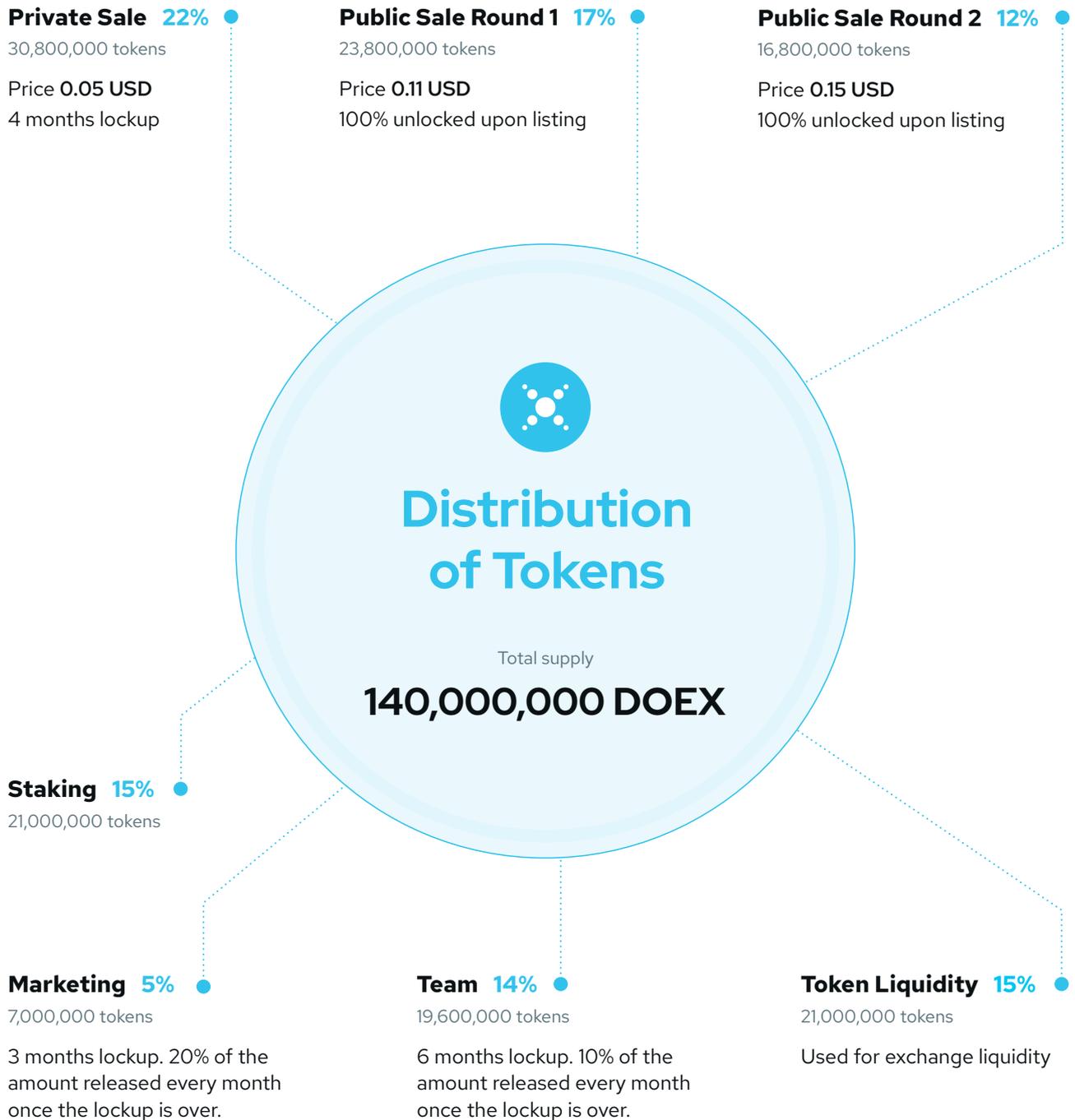
All | 1 Year | [90 Day](#) | 30 Day



Source: Defipulse

# TOKENOMICS

DOEX will issue 140 000 000 DOEX, native tokens on Cardano blockchain.



# FEATURES

Supports any Cardano native asset

Participate in liquidity pools to earn fees on ADA - Cardano Native Assets pairs

Automated pricing that is liquidity sensitive using AMM protocol

Trade ADA for any Native Token on the Cardano Blockchain

Trade any Cardano Native Token for another in a single transaction

Trade and transfer to a different wallet address in a single transaction

Purchase ADA or any other Cardano Native Token from Yoroi wallet

# UTILITY OF THE TOKEN

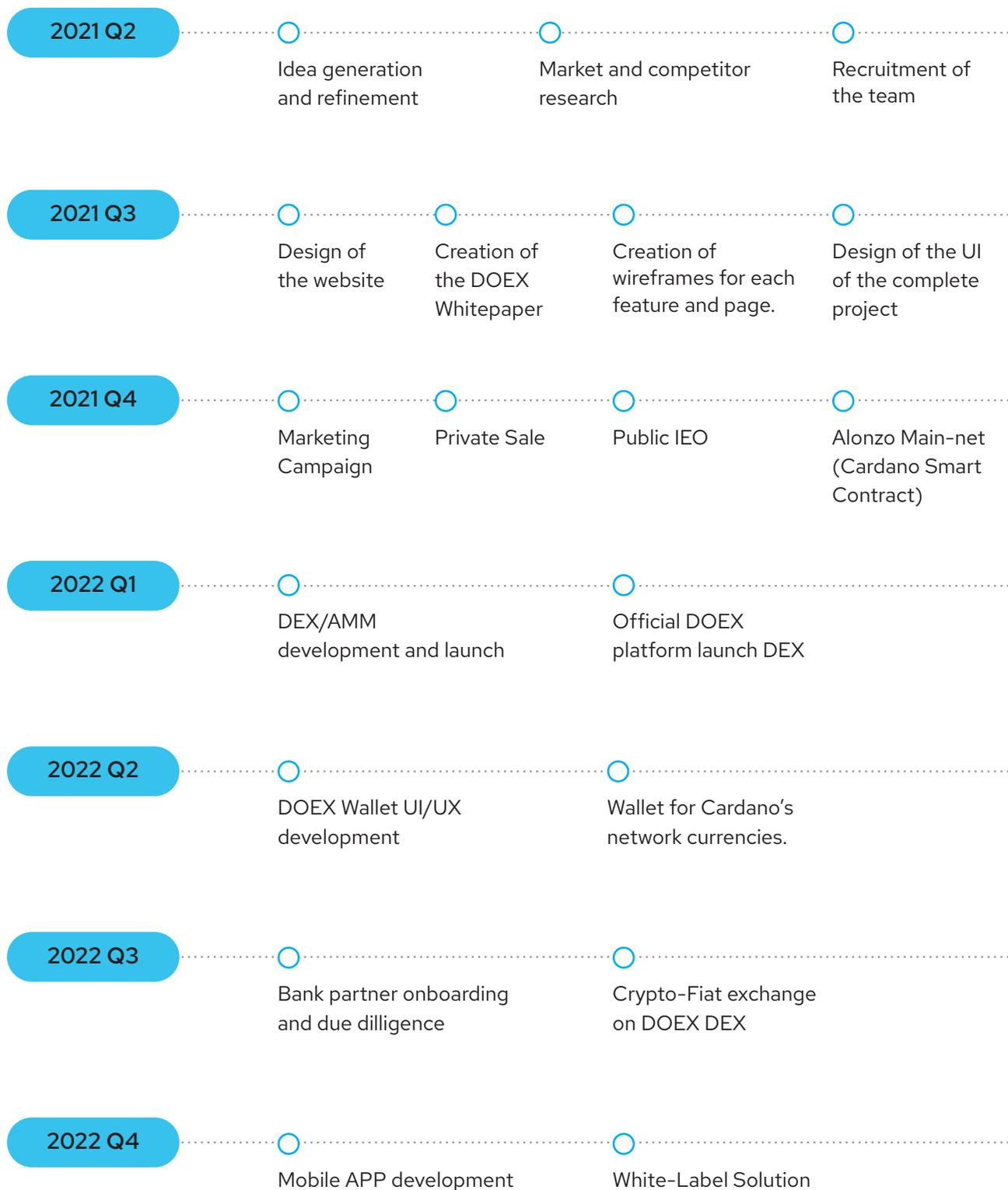
DOEX token is the native token of the DOEX platform and it is a utility token with several use cases that will drive adoption and increase its demand. Our aim is to make DOEX a truly decentralized, community driven protocol. For this purpose we have issued DOEX token with a voting function. Holders of the token will have voting rights and power based on the amount of tokens they have and will be able to debate, propose, and vote on all changes proposed to the DOEX platform. This allows the protocol to be upgraded by anybody with a good idea and they are incentivized accordingly.

According to available protocols, the common method that users employ to delegate their voting rights on proposals is by raising the relevant functions directly. For a proposal or function to go through and be accepted by the community, majority of the votes cast must be in favour. In a situation where there are more than two options, the proposal that has the highest votes wins. Platform users or community members will need to hold DOEX tokens to vote and it will be locked until the voting period ends.

## **A summary of the uses of DOEX token include:**

- Ability to cast votes and participate in the governance of the platform
- Incentivization of platform members
- Payment of fees such as Swap fees and slippage fees
- Participation in Liquidity Pool
- Payment of reward to Liquidity Providers

# ROADMAP



# DISCLAIMER

This paper is intended to convey general information only. It should not be taken as an investment advice or a solicitation or recommendation to take part in any investment and should not be used as a yardstick to evaluate the pros of making any investment decision. It should also not be taken to make accounting, legal or tax decisions or investment recommendations. This document shows current opinions of its authors and is not made on behalf of DOEX or their affiliates and staff. As such, it does not necessarily reflect what DOEX, their affiliates or individuals associated with them opines. The thoughts reflected herein are subject to change without prior notice.