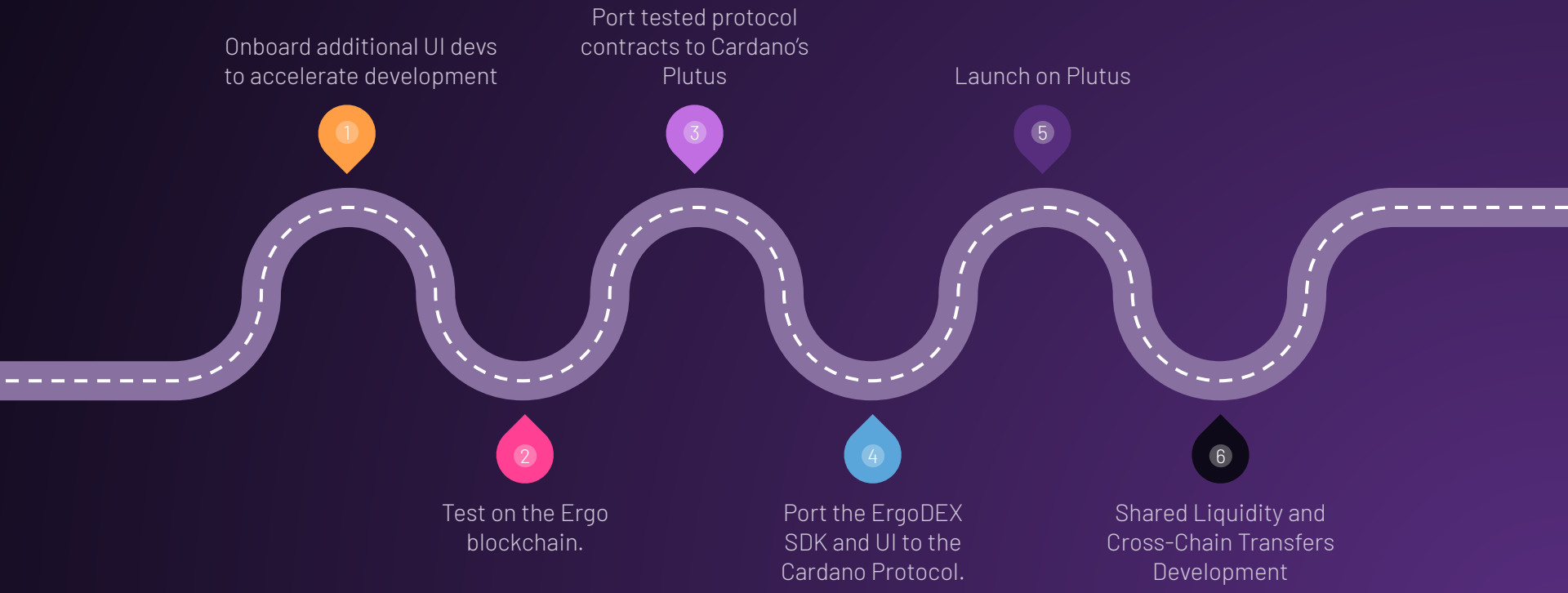
ErgoDex.io

INTRODUCTION

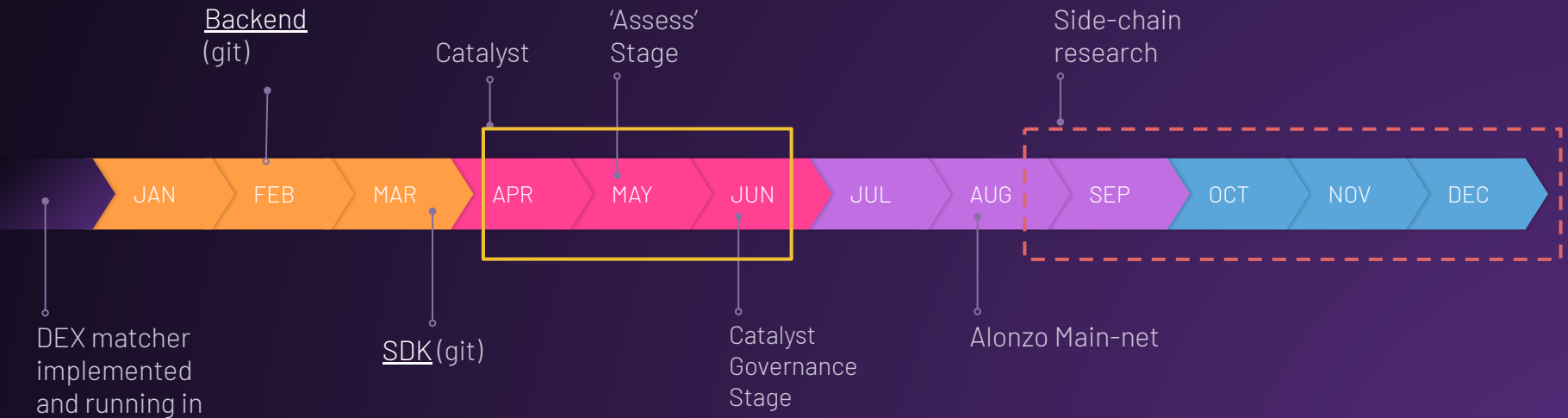
This presentation provides a description of the proposed **Automated Decentralized Exchange** protocol on top of Ergo and Cardano.

“It's one of the most revolutionary cryptocurrencies ever built. Got so many crazy ideas like sigma protocols and pruning the blockchain and roller chains. All this crazy stuff. Even has a proof of no premine. So really a technological marvel in many respects, and it reflects about 8 years of knowledge that Alex has amassed as both a researcher and a developer. Super concise code and it blows my mind that the market cap is where it's at. It should be a top 10 coin or top 15 coin.” - Charles Hoskinson

ROADMAP


Onboard additional UI devs to accelerate development
1
Test on the Ergo blockchain.
2
Port tested protocol contracts to Cardano's Plutus
3
Port the ErgoDEX SDK and UI to the Cardano Protocol.
4
Launch on Plutus
5
Shared Liquidity and Cross-Chain Transfers Development
6

TIMELINE


Backend (git)
Catalyst
'Assess' Stage
Side-chain research
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
DEX matcher implemented and running in the mainnet.
SDK (git)
Catalyst Governance Stage
Alonzo Main-net

BUSINESS MODEL CANVAS

Key Partners

Ergo partnered with Emurgo,

The commercial arm of Cardano to Promoting Interoperability. In their joint venture Ergo and Emurgo have released the following on the Ergo Blockchain.

1. Oracle Pools
2. The AgeUSD stablecoin protocol
3. Yoroi web
4. Yoroi dApp connector

Additionally, The draft AgeUSD Plutus contracts are available on the AgeUSD GitHub.

Key Activities

2020: Contract research and development started

Apr 2021:

DEX team is formed and serious development begins.

Ergo-dex-jdk is released

Base AMM UI development started.

Key Resources

Contracts, backend and SDK are all available on GitHub

- ErgoDex - Backend
- ergo-dex-sdk-js
- EIP14

Value Propositions

1. AMM DEX
2. AMM+Order Book DEX
3. Plutus port
4. Robust tokenomics
5. *Shared liquidity between Ergo and Cardano**
6. *Inter-chain swap protocol**

**Researched after working DEX is deployed to Plutus. Funded with remaining funds from this + DEX fee.*

Ergo's native programming language — aka ErgoScript — enables the development of Turing complete contracts that completely bypass the need for any gas fee while providing other peripheral benefits such as estimation of script complexity before execution, a facet that helps in the active prevention of DoS attacks.

More on what Ergo is bringing to Cardano here.

Key Point

Ergo is one of very few coins which has **fairness built-in**.

It had no;

Pre-mine, VC Funding or ICO. Supply is hard capped to 97.7 Millions ERGs

Dev-Channels

Upcoming Hackerthon in May, and an active Discord with community developers.

Ergo

eUTxO-based blockchain

Advanced DeFi

- *ErgoScript* (scala-like) for guard scripts
- Functional Programming
- Secondary Assets (NFTs, tokens)

Scalability

- Storage Rent
- Light-clients with full-node security
- NiPoPows

Smart Contracts for the People

Cost Structure

- 3 UI devs full time remote, 3 month: 45K$
- ErgoDEX UI design: $10k - *Core development (Port of contracts, SDK and backend update)*
- 2 devs full time, 2 month: $30k
- ***Any remaining funds will be dedicated to a research of inter-chain Ergo-Cardano liquidity transfer.***

Revenue Streams

There are three types of economic agents in the ErgoDex ecosystem, each is incentivised to fulfil their role as completely as possible. See the Tokenomics section for more information.

Protocol Architecture

Thanks to the eUTXO model, liquidity pool contracts for AMM-based DEXes can be combined with order contracts.

This gives unique possibility to have shared liquidity among different types of exchanges on top of the Ergo and Cardano blockchains.

PROTOCOL ARCHITECTURE : ORDER-BOOK DEX

Traders benefit from DEX services they use

Orders are waiting for another orders to be matched, or for a cancellation.

There're the following three types of orders —

1. "buy" (i.e. buy tokens for native asset),
2. "sell" (i.e. sell tokens for native asset),
3. "swap" (buy tokens for other tokens) orders

An Order-book DEX has the advantage of working best for those pairs with high liquidity.

Atomic limit orders

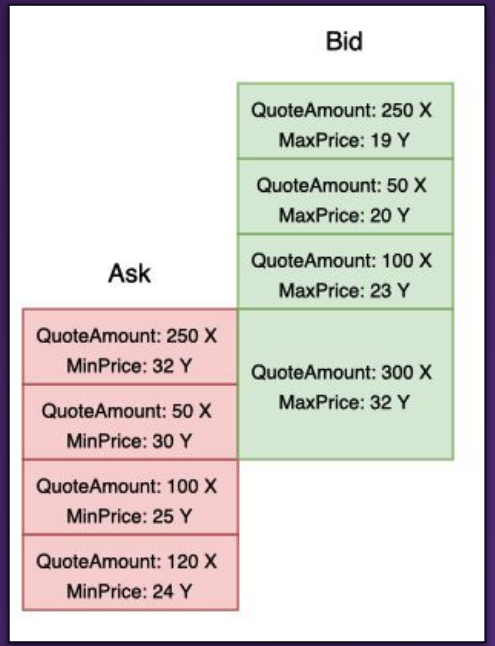
Atomic orders can only be executed completely and are otherwise refunded.

Such orders can either be aggregated by the ErgoDEX client so that users can choose from them or matched in an order-book with partial orders which will be defined next.

Partial limit orders

Partial orders are something more familiar to those who've ever used *classical* centralised exchanges. (CEXs)

These orders can be partially executed, meaning the best way to work with them is an order-book, where they can be aggregated, matched and executed by ErgoDEX bots.



PROTOCOL ARCHITECTURE : AMM DEX

Unlike an order-book based DEX which rely on an order-book to represent liquidity and determine prices, AMM DEXes uses an automated market maker mechanism to provide instant feedback on rates and slippage.

AMM best suits pairs with low liquidity.
Each AMM liquidity pool is a trading venue for a pair of assets.
In order to facilitate trades a liquidity pool accepts deposits of underlying assets proportional to their price rates.

Whenever deposit happens a proportional amount of unique tokens known as liquidity tokens is minted. Minted liquidity tokens are distributed among liquidity providers proportional to their deposits. Liquidity providers can later exchange their liquidity tokens share for a proportional amount of underlying reserves.

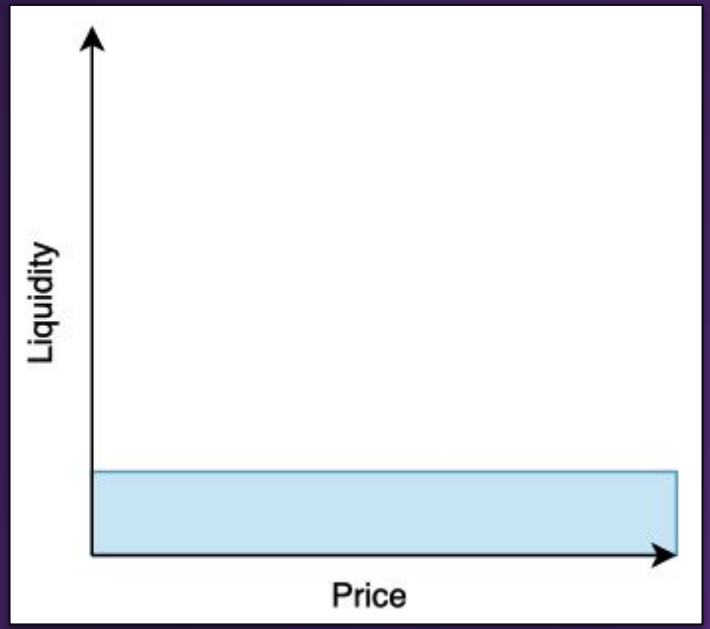
PROTOCOL ARCHITECTURE : AMM DEX

Constant Function Market Makers

CFMM (classical AMM pools) are based on the Constant Product formula; **x*y=c**,

where **x** and **y** are deposits on tokens **X** and **Y** respectively, and **c** is their product which remains constant after swap operations.

CFMMs provide liquidity across the entire price range.



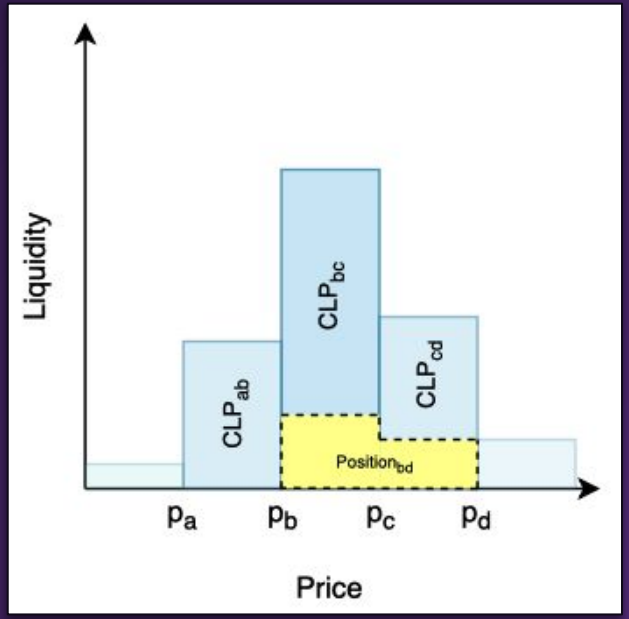
PROTOCOL ARCHITECTURE : AMM DEX

Concentrated AMM pools

While in CFMMs, liquidity is uniformly distributed along the reserve curve, this can be slightly inefficient as much of the reserves held in a pool are never used. **Concentrated AMMs allow LPs to provide liquidity to smaller price ranges.** Each pair is composed of smaller pools, each corresponding to some price range.

We call such pool a Concentrated Liquidity Pool (CLP).

A CLP only needs to maintain enough reserves to support trading within its range, and therefore can act like a constant product pool with larger reserves (we call these the virtual reserves) within that range. At the same time LPs are not bound to some particular CLP and price range and can provide liquidity to multiple adjacent CLPs therefore forming something what we call a position. While price of an asset is within a position's price range the position is earning protocol fees. When the price escapes the position's price range it's liquidity no longer earns fees as it's not active anymore.



TOKENOMICS

We incentivize each actor to fulfill their role as best as possible.

TOKENOMICS

There are **three** types of economic agents in the ErgoDEX ecosystem.

1. DEXes

Parties which run DEX bots and UI need to be incentivized in order to provide best services. **DEXes earn fees from both OrderBook and AMM services**

In **AMM**:

1. Fees are charged for every operation on a liquidity pool
2. An amount of native tokens defined by a user for deposit|redeem operations
3. An amount of native tokens defined by a user for each unit of quote asset exchanged

In **OrderBook**:

1. Fees are charged in native tokens for each unit of quote asset exchanged

2. Traders

Traders benefit from DEX services they use

3. Liquidity Providers

LPs benefit from protocol fees paid in tokens and accumulated in liquidity pools.

A new unique token pair called "LP token" is issued. For full details please see EIP-14

TEAM

Team has a solid background in core and ecosystem development with projects including Ergo and Scorex.

Ilya Oskin
Ergo Core Developer

Lead Developer at Mail.ru Group.

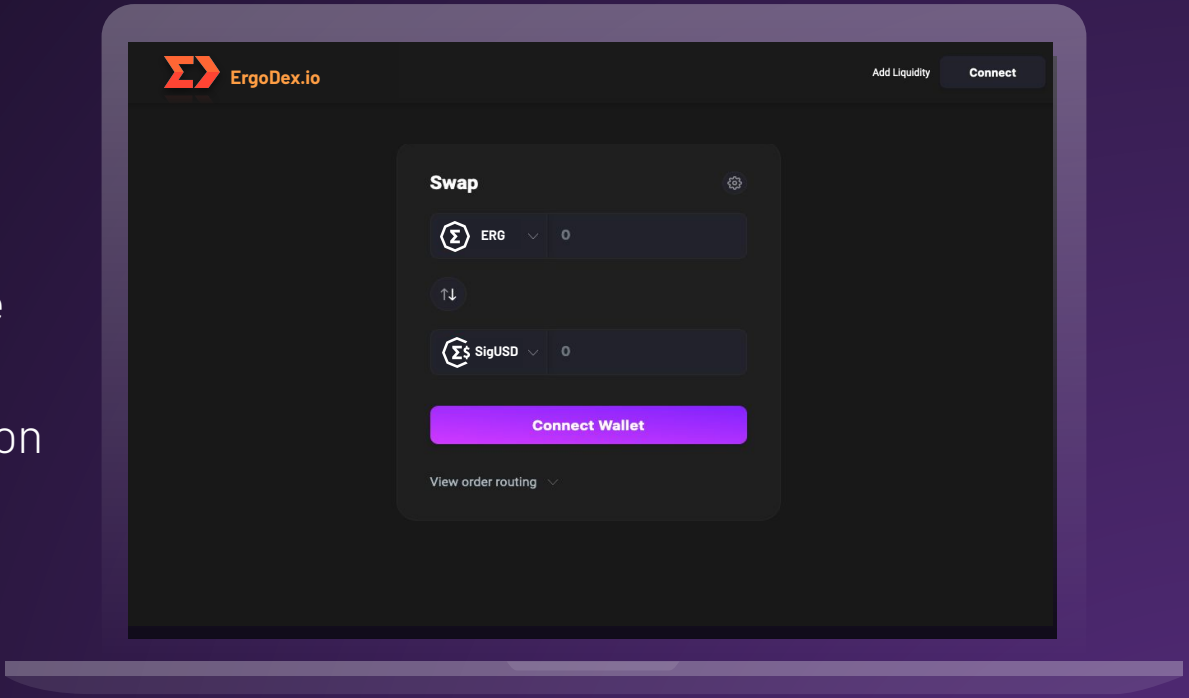
Dmitry Usov
Ergo Developer

ex. Frontend Team Lead at Citymobil, Javascript developer at Chatfuel.

AMM APP

Step 1.

Minimal Viable Product implemented on the Ergo Blockchain



More advanced DEX to follow, similar to other Order-Book style centralised exchanges (Binance, CoinEx, etc).
With the ultimate goal of having one interface, allowing the user to switch between Ergo & Cardano.

Once this functionality is done, we will start working on shared markets between Ergo & Cardano, cross-chain gateways, sidechains, and more !

FIND OUT MORE

Please vote for us Ideascale!

r/ergonauts

ergoplatform

- Technical protocol description
- Non-tech protocol overview
- ErgoDEX SDK
- Trustless matcher bots