eckoDEX

Litepaper

dex.ecko.finance

Table Of Content

Abstract

In this day and age, all Decentralised Exchanges (DEXes) suffer from the same lack of usability, driven by gas costs and vulnerability of protocols. This issue limits users that want to partake in trading and providing liquidity to those with financial or technical ability. In order to ensure a truly open marketplace which anyone can participate in – the ultimate Decentralised Finance (DeFi) promise – a solution must be created to lower financial barriers of entry and to reduce inefficiencies that are detrimental to traders.

eckoDEX achieves exactly this by building the first DEX built upon Kadena, the first truly scalable Proof-of-Work (PoW) layer-1 blockchain network and utilizing the same Automated Market Maker (AMM) model as Uniswap. Through the power of Kadena's braided chain framework, the possibility of Miner Extracted Value (MEV), frontrunning and gas auctions is all greatly reduced, ensuring faster and cheaper transactions in the process, while being settled by the globalized security that only PoW can provide. Kadena also offers the paradigm-changing ability to offload gas payments to a third party via gas stations. This enables eckoDEX to deliver a gas-free liquidity pooling and trading experience while also allowing for novel approaches to liquidity provisioning and slippage controls.

Besides the technical advantages brought to DeFi, eckoDEX introduces its utility token - KDX - to establish true democracy and community ownership of eckoDEX's ecosystem and to implement the first financially sustainable Liquidity Mining programme. This allows the community to steer the development of the platform, achieving a collective vision, while also incentivising participation in certain pairs, and therefore improving the overall users swapping experience.

All together, these technologies create a DEX and a DeFi tool suite that is positioned to not only support the Kadena ecosystem, but to create DeFi in the way it was supposed to be: open to all, community owned, simple to use and cheap to participate in.

1. Why eckoDEX

eckoDEX's innovation is defined by the juxtaposition of the current state of DeFi; by the costs and trade-offs accepted by its users. To understand the depth of what eckoDEX achieves, we must first understand the shortcomings of the current DeFi ecosystem.

At a high level, Kadena's multi-chain driven scalability with eckoDEX gas stations means:

Table 1 – eckoDEX competitive advantages

No gas costs	Subsidized by eckoDEX through gas stations
No gas prioritization	No mempool[1] queues
Lightning-fast trades	On a Layer-1 blockchain
PoW security	Made stronger with braided chains
Infinitely scalable	Able to meet any future throughput demand
Fair token launch	No Venture Capital investors (VCs) involved
Liquidity mining 2.0	Sustainable KDX rewards emission
Run by a DAO	Truly democratic and open to all

1.1 Problems In DeFi

The problems currently plaguing today's DEXes are, for the most part, not caused by any technology issues specific to the platforms themselves. The reason why people do not trade on them or do not lend them their liquidity lies in the high gas costs associated with doing so. At the time of this paper, an average Ethereum-based DEX user would find transaction fees unsustainable for small and medium size tickets. This makes it not practical for small trades and it creates limits on who can participate and make use of the decentralised finance promises.

Unfortunately, these scalability and gas-driven problems bring in some unintended consequences, such as bots and miners reprioritizing or creating transactions that benefit from market movement at the cost of the average user. In order to fix many of these issues, blockchain networks have been moving toward different security models: opting for PoS as a solution to increase scalability and speed, while lowering transaction costs. This has worked in some ways but still faces the same PoW challenges. As adoption grows, the network gets congested and consequently causes increasing transaction costs.

---

[1] In blockchain terminology, a mempool is a waiting area for the transactions that haven't been added to a block and are still unconfirmed. This is how blockchain nodes manage and order transactions that have not yet been included in a block

At the same time, security levels are sub-optimal compared to PoW networks that provide provable financial security. Ultimately, it seemed impossible to simultaneously have scalability, speed and security.

Kadena has proven to be the only blockchain able to solve this infamous trilemma.

1.2 Solution: Long Term Scalability

One of the keys to solving the trilemma is in achieving long term scalability. Many projects proport scalability with their low transactional costs, only to see them rise with adoption. Kadena is the first and only PoW Layer-1 blockchain that has managed to permanently address scalability, accomplishing what all others (such as BTC and ETH) have failed to.

Kadena's Layer-1 blockchain protocol, Chainweb, functions as a braided blockchain data structure, progressed via a parallelized consensus mechanism; a unique architecture that enables infinite scalability while preserving the power of PoW security without sacrificing decentralisation. This framework minimizes the number of hops to get to the farthest chain (referred to as diameter) and the number of edges (the hashes that link the blocks from other chains – referred to as degree). This minimizes the network overhead required to maintain a completely linked structure of chains. In 2021, Kadena successfully expanded from 10 to 20 chains. This 20-chain configuration (as shown below) has degree 3 and diameter 3. Therefore, a wait time of only 3 blocks is required after a transaction confirmation before the whole network's hash power is securing it. After 3 blocks, coins are considered fully confirmed and can be transferred from one chain to any other chain.

Figure 1 – Kadena Chainweb Scalability
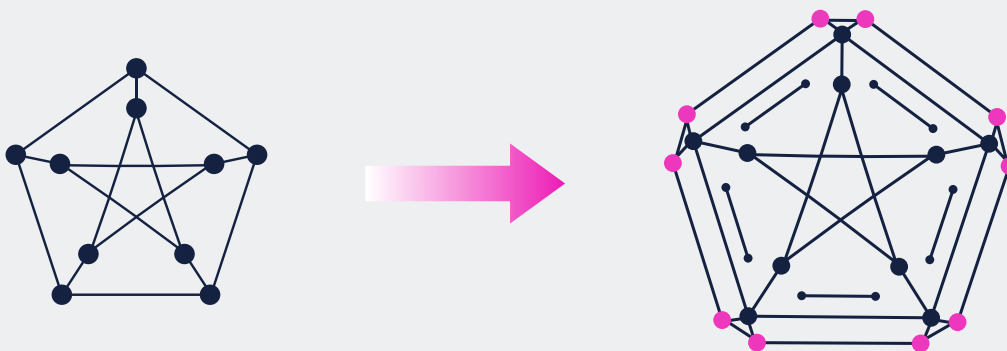
By leveraging this breakthrough technology and infrastructure, eckoDEX can truly satisfy any throughput demand, being the first infinitely scalable and secure DEX. eckoDEX will not face any risk of market congestion by users' activity or volume and can instead focus on technologies that increase profitability to users.

1.3 Solution: Gas-Free

Kadena, through the novel concept of gas stations, offers the ability to specify a gas payer for smart contract interactions. This allows eckoDEX to subsidize all gas fees while interacting with our DEX. That's right, gas free, forever, whether you are adding or removing liquidity or swapping. No longer will users be required to have a separate token to pay gas or even consider gas costs when using the DEX.

1.4 Solution: Slippage Control

The gas problem affects more than just performance and economics. Miner Extracted Value, frontrunning and gas auctions all take advantage of the underlying blockchain's inability to properly scale in order to take advantage of users and their trades. This often results in massive amounts of gas being spent to eke out every bit of profit opportunity, failing users' transactions in their wake. Users then worry more about the cost of their transactions failing than their want to trade.

Kadena, with its multichain architecture, offers a unique opportunity to minimize this into oblivion by being able to scale any time there is a threat of mempool queues. eckoDEX uses this to create a DEX with no transaction wait times (lightning fast), giving little opportunity for others to frontrun, increasing the success rate of trades, while giving the users industry leading slippage control to maximize profit.

1.5 Solution: Decentralised Infrastructure

eckoDEX believes in the true vision of DeFi: decentralise everything and open to all. From liquidity provisioning, pricing to swapping, to ownership and organization, to websites and front-ends - if it can be run on-chain, it is; if it can't, then we ensure there is no central authority or service.
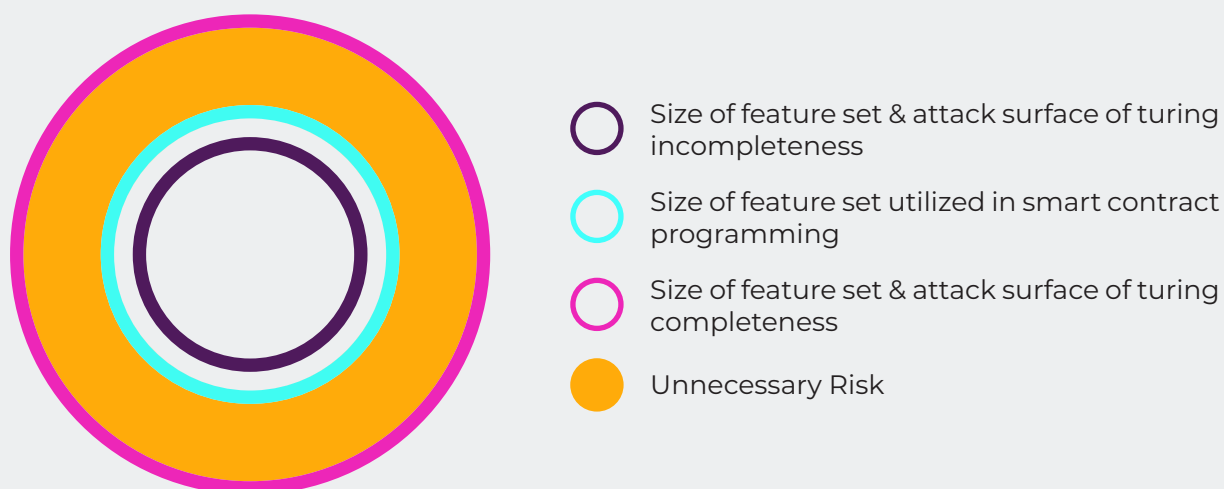
This idea is often brought to the very edge with not actually going all the way, with DEXes maintaining control of their interface and centrally hosting their website and front-end. Not eckoDEX. From our website and front end being hosted on Flux, to everything in our eckoDEX code being owned by the DAO, we are DeFi.

1.6 Solution: Secure Smart Contracts

Half of the time DeFi is in the news is because of hack that has caused a massive leak of funds from a DeFi protocol. No matter the size of the attack and whether or not it was fixed, the project and protocol never recover. Many of these vulnerabilities are direct consequence of the language they were developed in, Solidity, being Turing complete.

Turing completeness describes the ability of the language to express all tasks accomplishable by computers. This sounds powerful in theory, creating no bounds to what could be done on the blockchain (if we ignore gas). But what started as a powerful idea has actually turned into a problem. With this open-ended ability came hard to anticipate attack vectors. To date, there are 16 known attack vectors in Solidity, which much of the DeFi ecosystem is built upon, most of which would not be possible if Solidity was Turing incomplete.

Figure 2 – Unnecessary risk associated with turing completeness

○ Size of feature set & attack surface of turing incompleteness

○ Size of feature set utilized in smart contract programming

○ Size of feature set & attack surface of turing completeness

● Unnecessary Risk

Kadena's smart contract language, Pact, seeks to improve on this problem by designing a language with the known limitations of blockchain in mind, resulting in a Turing incomplete language that is purpose driven to produce easy to read, secure and efficient smart contracts. This is amplified by the built-in support of formal verification, giving developers immediate feedback on possible bugs that would otherwise go unnoticed. This overlooked detail ensures eckoDEX will be not only secure transactionally via PoW but also secure from attack.

2. Industry Outlook

Decentralised Finance has been growing at an explosive rate with most of the developments and new projects being small incremental improvements upon broken systems that are institutionalizing inefficiencies that drive high cost and risk to users. Despite all this, the DeFi industry continues to grow. This mix of ecosystem growth with fundamental technological gaps create a perfect opportunity for eckoDEX to deliver a solution that will change the course of DeFi.

2.1 DEX Market Potential

Market data shows that since the so-called DeFi Summer of 2020, decentralised finance has become increasingly mainstream. The considerable amount of volume traded on DEXes highlights the opportunity that eckoDEX faces, a project that not only addresses the weaknesses and deficiencies of the traditional financial industry, but also those of eckoDEX's existing competitors.

DeFi is still in the early stages of existence. However, as of October 2020, over $11 billion was deposited across multiple decentralised finance protocols – a figure that represents a more than tenfold growth over the course of 2020. In the wake of this explosive trend, Nasdaq decided to create a stock market index (DEFX) to keep track of the largest DeFi products. There are currently about 200 DeFi projects, 90% of which use the Ethereum network.

Figure 2 – Total Value Locked in DeFi Protocols
defillama 20.12.2021

Total TVL
$234.43B +0.34%

Since January 2020, DEXes yearly volume have experienced an over 2,000% increase, currently accounting for $4.2 billion in swap fees. These numbers show that investors have a strong forward-looking interest in DEXes and possible alternatives to traditional finance.

2.2 eckoDEX: The Next Generation Of DEXes

Many of eckoDEX's competitors, namely those that proport the same benefits in cost and scalability, are based on PoS blockchain technologies. In such systems, transactions are validated based on tokens owned and staked on the blockchain. Thus, by its very nature, PoS tends to centralise tokens in the hands of very large nodes (either directly or via delegation). In general, centralisation means efficiency, but it goes against the original fundamental blockchain philosophy of decentralisation and disintermediation. PoS is not substantially different from the way fiat money systems work, wherein major stakeholders have a quasi-monopoly control over the whole system. Actors with larger deposits hold the responsibility for controlling how transactions are validated and how much new money is created (concentration dominance).

The possible involvement of financial institutions in PoS-based blockchains is a tangible risk and is ultimately the reason why PoS does not work. It essentially pays the rich to be rich and functions as an authorization-based system – therefore not decentralised. The integrity of a blockchain network relies on total decentralisation and the PoS model currently undermines this quality.

PoW, on the other hand, has been used extensively for a decade, showing itself to be provably secure as a function of the amount of computing power required to influence the network. This inherently means that PoS and PoW do not hold the same level of confidence and reliability. The risk of hacking and cyber-attacks is a factor that cannot be overlooked when discussing blockchain security. To date, there have been a total of 54 relevant hacking events, with funds lost totaling at around $2.4 billion at the time of these hacks.[2]

The origins and rise of PoS projects are linked to a fundamental technological deficiency of PoW Layer-1 blockchains. Before Kadena, no blockchain had been able to offer a secure, decentralised platform that solved the problem of scalability. This left room for temporary tactical solutions that never fully addressed the core issues. Now because of Kadena, users benefit from a blockchain network that provides all the advantages of PoW consensus, while being infinitely scalable and maintaining decentralisation.

[2] Cryptosec.info/exchange-hacks (20.12.2021)

It is this ability to scale along with novel improvements to smart contract logic that enables eckoDEX to bring the security of PoW in a scalable and gas-free environment to DeFi. This strong departure from the traditional Ethereum based model will revolutionise the face of DeFi, delivering tools that are truly open and accessible to all.

Table 1 – Average fees for swaps on different DEXes when running on Ethereum
Crypto.com - 17.12.2021.

DEX	Blockchain	Gas Fees
eckoDEX	**Kadena**	**$0**
Uniswap V2	Ethereum	$66.17
SushiSwap	Ethereum	$59.17
Curve	Ethereum	$47.08
Mooniswap	Ethereum	$62.49
Balancer	Ethereum	$86.28

3. Tokenomics

KDX is eckoDEX's utility token – a programmatic scarce resource with a limited supply of 1 billion tokens – that enables eckoDEX to enforce decentralised governance and to attract LPs. DAO contributors can take advantage of the large portion of allocated token to enhance DAO participation through grants and bounties, and to, in parallel, grow the network and swap volume. Additionally, KDX holders can stake their tokens to claim 0.05% of every swap, proportionally to the KDX stake owned. KDX liquidity mining programme aims at incentivising users' participation and deepening pools' liquidity, while at the same time keeping the KDX vesting schedule predictable and sustainable in the long term.

3.1 KDX Distribution

Team – 5%

Team tokens only account for 5% of KDX total supply, in order to strengthen the overall decentralisation and to ensure long term market stability of the KDX token. Team tokens have a rigid unlocking schedule[3] to avoid any risk of market flooding in the delicate infant phase of the DEX.

Burned – 10%

A significant portion of the total token supply of KDX has been burned with the aim of enhancing the overall scarcity of the token. This strategic decision was made to benefit very first KDX supporters and to create a more robust token economy.

Community Sales – 20%

Tokens allocated to the community sales account for 20% of the overall supply, in order to empower network participants from the start and to guarantee an organic and decentralised platform growth. At the same time, the large allocation dedicated to early supporters is crucial to finance eckoDEX development and operations.

Community Rewards – 25%

Community Rewards account for 25% of the KDX supply, in order to guarantee users a long-term DAO and community-led vision. The DAO will fund future operations and developments - in a completely decentralised fashion – through the deployment of grants and bounties, open to everyone. Community initiatives range from ecosystem growth, Tokenomics impulse, marketing, IT and Smart Contract (SC) development and anything related to long-term eckoDEX success.

Network Rewards – 40%

Network Rewards account for 40% of the KDX total supply, in order to attract users, LPs and investors. In eckoDEX, users are empowered through gas-free transactions, while LPs are incentivised via a programmatic emission schedule of rewards to be claimed in KDX as a booster. In this way, KDX inflation rate can be controlled and adjusted according to market participation: measured by Volume and Total Value Locked (TVL) in the platform.

[3] 2nd year: 50% - 3rd year: 75% - 4th year: 100%

3.2 KDX Liquidity Mining 2.0

Liquidity Mining – the process of attracting liquidity through distribution of native KDX tokens – is at the core of eckoDEX's success. eckoDEX technology allows users to swap instantaneously with no gas costs nor additional fees. Therefore, this creates an unprecedented incentive for users to come and trade on eckoDEX. On the other hand, KDX Tokenomics – with the larger portion of tokens allocated for network rewards (40%) – can generate lucrative pool boosters for early LPs.

Many DEXes in the industry have failed by creating a non-sustainable relationship between the inflation rate – emission schedule of rewards in eckoDEX case - and token demand. eckoDEX tackles this issue by initially allocating only 5% of tokens to the core team, meaning that a larger portion of incentives can be later distributed to LPs. Additionally, the rewards emission schedule of KDX is programmatic and self-adjusting according to market conditions..

The DEX industry has seen many projects quickly disappear after consuming all their liquidity incentives. Naturally, the end of extra incentives for LPs leads to a loss in the overall value of the DEX, as LPs will just migrate to the new and more lucrative options. This results in a difficult multivariate equation of attracting liquidity (with higher incentives) and implementing a sustainable rewards emission schedule. eckoDEX solves this multivariate equation by being both lucrative and sustainable. Lucrative for LPs with a logarithmic programmatic vesting schedule to distribute extra incentives and Sustainable as users are economically driven to swap where it is free, fast and secure.

4. Vision

The world of DeFi has proven to be the first tangible and concrete blockchain use-case. Various projects have developed a vast and innovative ecosystem of technologies that have quickly outpaced Traditional and Centralised Finance solutions (CeFi).

eckoDEX exists to deliver the true vision of decentralised finance by creating financial tools that are accessible to all and entirely decentralised. This means accessibility in cost and simplicity, decentralisation of everything from the website and swap platform, to the establishing of the DAO that is created to take it all over, to creating sustainable liquidity mining programs. Achieving this vision goes well beyond the first version of eckoDEX as a gas-free DEX platform and is about positioning eckoDEX to scale toward future adoption and to provide tools and technologies that propel DeFi, as an ecosystem, forward.

Kadena, with its multichain framework paired with gas stations arms eckoDEX with the ability to create novel scaling technologies that provide fine grained liquidity provisioning and slippage controls that reduce risk and increase profitability for all users, all while maintaining fast and gas-free transactions. These technologies will be part of future iterations of the eckoDEX DEX.

Beyond the initial V1 of the swap platform, eckoDEX will be expanding the DeFi tool suite to include a professional trading platform, analytics tools, and a lending platform, all in the name of delivering tools to satisfy every need and to onboard both retail and institutional parties, on the most decentralised DeFi platform, built upon the only scalable PoW layer-1 blockchain, Kadena. These technologies will make Kadena the home of DeFi, and eckoDEX the leader of the space.

Annex

Definition Table

Acronym	Name	Definition
AMM	Automated Market Maker	AMMs allow digital assets to be traded without permission and automatically by using liquidity pools instead of a traditional market of buyers and sellers.
DAO	Decentralized Autonomous Organization	A DAO is a blockchain-based organization that is democratically managed by members through self-enforcing open-source code and typically formalized by smart contracts. DAOs lack centralised management structures. All decisions are voted upon by network stakeholders. DAOs often utilize a native utility token to incentivise network participation and allocate proportional voting power to stakeholders based on the size of their stake. As DAOs are built on top of blockchains, their transactions are executed transparently on the underlying blockchain.
dApps	Decentralised Applications	dApps make use of blockchain technology to address use cases ranging from investment to lending to gaming and governance. Although dApps may appear similar to web applications in terms of user experience, dApp back-end processes eschew centralised servers to transact in a distributed and peer-to-peer fashion. Rather than using the central Hypertext Transfer Protocol (HTTP) to communicate, dApps rely on wallet software to interact with automated smart contracts on networks.
DeFi	Decentralised Finance	DeFi is a major growth sector in blockchain that offers peer-to-peer financial services and technologies built on blockchain technologies. DeFi exchanges, loans, investments, and tokens are significantly more transparent, permissionless, trustless, and interoperable than traditional financial services, and trend towards decentralised governance organizational methods that foster equitable stakeholder ownership.
DEXes	Decentralized Exchanges	A DEX is a financial services platform for buying, trading, and selling digital assets. On a DEX, users transact directly and peer-to-peer on the blockchain without a centralised intermediary. DEXes do not serve as custodians of users' funds and are often democratically managed with decentralised governance organization. Without a central authority charging fees for services, DEXes tend to be cheaper than their centralised counterparts.
KDX	EckoDEX Token	KDX is the native eckoDEX utility token and has a fixed supply of 1 billion tokens. KDX is used to incentivise all the liquidity stakeholders on the eckoDEX platform, while also rewarding its holders for supporting the network.

LPs	Liquidity Providers	A LP is a user who deposits tokens into a liquidity pool. In return for supplying liquidity, users are typically awarded LP-tokens that represent the share of the liquidity pool the user owns.
MEV	Miner Extract-ed Value	MEV is a measure of the profit a miner (or validator, sequencer, etc.) can make through their ability to arbitrarily include, ex-clude, or re-order transactions within the blocks they produce.
PoS	Proof of Stake	PoS is emerging as one of the most widely used blockchain consensus mechanisms. PoS networks incentivise participants to stake native coins in a network of validator nodes. Upon the close of a transaction block, validator nodes are eligible to be randomly chosen to validate block data, thus generating the subsequent block, and earning native coins as a reward. A ro-bust nodal network offers increased network security, resiliency, and computational power. PoS systems also generally enable validator nodes to contribute democratically to decentralised platform governance through voting on key updates and deci-sions.
PoW	Proof of Work	PoW is a blockchain consensus mechanism first popularized by the Bitcoin blockchain network. PoW systems rely on a process of mining to maintain the network. Miners provide computer hardware that competes to solve the complex cryptographic puzzles required to confirm data transacted on the network and are rewarded for doing so with the network's underlying cryptographic token for doing so. PoW blockchain systems are decentralised and secure as compared to other network consensus methodologies, but typically struggle to achieve the network scalability needed for widespread global enterprise adoption.
TVL	Total Value Locked	TVL is a metric that measures the aggregate value of all crypto assets locked in decentralised finance protocols via smart con-tracts. It was popularized by DeFi Pulse in 2019, but with price data that goes back to DeFi's genesis in 2017. TVL can also refer to the amount locked on a specific protocol (such as Aave or Uniswap). TVL data can also be further broken down and mea-sure the DeFi value locked by purpose or type (such as lending and derivatives).
UI	User Interface	UI is the point at which human users interact with a computer, website or application. The goal of effective UI is to make the user's experience easy and intuitive, requiring minimum effort on the user's part to receive maximum desired outcome.
UX	User Experi-ence	UX encompasses all aspects of the end-user's interaction with a company, its services, and products. UX design is mainly con-cerned with the user's expectations. The ultimate goal of UX is to locate and solve problems customers are struggling with.

VCs	Venture Cap-ital	VC is a type of private equity financing that is provided by a venture capital firm to start-up businesses that are deemed to have high growth potential. VC is usually provided by high net-worth individuals (HNWIs), investment banks, or large enterprises that invest in a specific industry. Often VC firms specializing in blockchain only invest in startups that are designing blockchain-specific businesses. Venture capital funding also sometimes entails technical or managerial expertise. VC firms often provide funds to companies during their initial stages, such as seed round funding.