duckpools

Protocol Whitepaper

hello@duckpools.io

January 24 2023
v1.1

1 Introduction

duckpools is a pool-based lending protocol that made its debut in the Ergo ecosystem on July 31, 2022. Within 4 months of its creation, *duckpools* delivered a working beta and became the first decentralized application (dApp) on Ergo to facilitate lending and collateralized borrowing of ERG and its native assets.

As a pool-based lending protocol, lenders can deposit cryptocurrencies to a pool contract to passively earn income on their assets and borrowers can borrow cryptocurrencies from the pool by placing a collateral. Loans do not need to be individually matched; instead, they are funded using pooled funds, secured by a borrower's collateral. This allows for instant, perpetual loans with loan conditions such as the interest rate and liquidation conditions dictated by the state of the pool.

1.1 Project Inception

Throughout 2022, it became apparent to us that despite the underlying power of the Ergo blockchain and its expressive smart contract language Ergoscript, the Ergo DeFi ecosystem was being outshined by mainstream blockchains on the sheer size of its userbase. We created *duckpools* because we believe a lending protocol can act as a *catalyst for explosive growth* within the Ergo DeFi space. *duckpools* was built not only to *highlight* Ergo's existing DeFi protocols but also to become a staple product in its own right. We believe a lending protocol like *duckpools* can enrich the current ecosystem and become the foundation for new, undiscovered financial products to prosper in the Ergo space.

1.2 Why Ergo?

We firmly believe that developing decentralized applications on Ergo is simpler, faster, and more scalable than on any other blockchain. As detailed in our comprehensive *Feature Development Budget*, we believe *duckpools* can become competitive or even functionally superior to leading market competitors across the entire crypto space, *for a fraction of the development cost.* This is not a testament to our process or team; we believe it is Ergo's robust and innovative design that makes this possible. We expect that *duckpools* can become the success story that onboards prospective developers and investors to the Ergo ecosystem.

2 Project Architecture

This section provides a high-level description of the *duckpools* protocol and offers comments on its current properties and design. For a more technical overview, we encourage readers to view our Github where our open-source smart contract code is stored alongside some protocol descriptions.

2.1 Lending Pool Structure

duckpools, as a pool-based lending protocol, generates yield for lenders on an asset they lend to a pool and allows borrowers to instantly borrow from the pool by supplying some collateral. Consequently, on an UTxO-model chain

like Ergo, it is most natural to represent a lending pool as a single UTxO; this is the design choice we have made for the protocol. In this way, all lender funds are stored as one box on-chain, and as such, the state size of the protocol is minimal. With a single UtxO representing a lending pool, pool utilization levels (the ratio of borrowed to unborrowed funds) can be easily determined, which allows for the efficient calculation of variable interest rates. Furthermore, this method simplifies risk assessment which enables secure and efficient auditing processes.

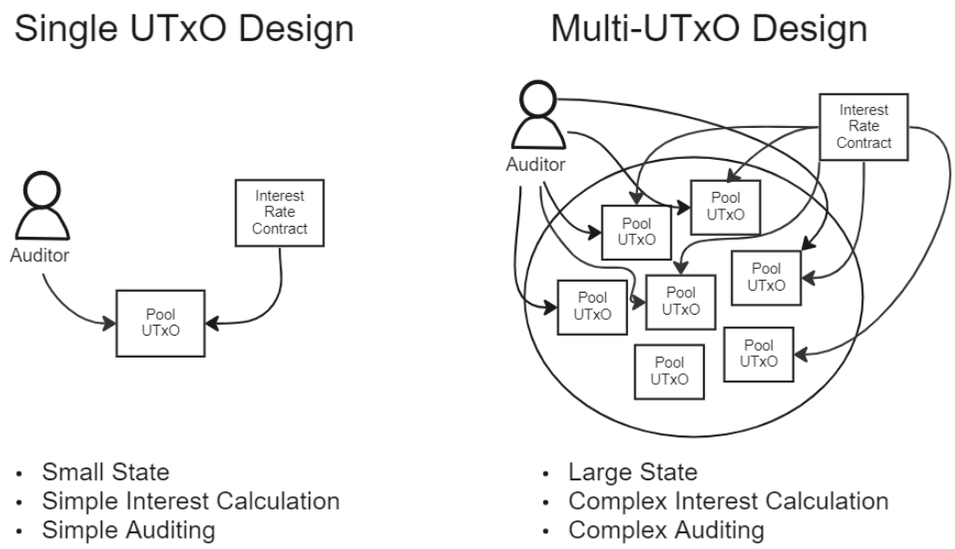

Figure 1: Single UTxO vs Multi-UTxO Design

Every lending pool on the protocol is bootstrapped with its own *Lender Token*, which is a token that is used to represent a lender's share of assets in a lending pool. Just like any other Ergo native asset, these tokens can be traded, sold, or used as collateral for loans on *duckpools*. Most importantly, lenders and borrowers always have custody over their funds; any deposits into the protocol are secured by decentralized smart contracts that can only be unlocked using the borrower's *private key* or the lender's *Lender Tokens*. For scaling, both borrowers and lenders interact with the pool using *proxy contracts*, which are contracts that are chained together using off-chain bots that carry out user orders.

The *duckpools* protocol aims to be a risk-averse protocol for lenders and as such, all smart contracts are designed such that the value of the *Lender Token* cannot decrease. Furthermore, all loans are overcollateralized and current pools are designed with conservative liquidation thresholds. In practice, extreme market factors or smart contract bugs make it *possible* for the value of the *Lender Token* to decrease; however, ultimately, the platform gravitates toward low-risk design practices.

In its current form, lending pools are segregated based on the asset offered to borrowers. Whilst pools are free to select a bucket of assets to be accepted as forms of collateral for loans, only one asset can be borrowed or loaned to a single pool. This allows for the permissionless formation of new pools when new cryptocurrencies are created and simplifies risk assessment for lenders.

In practice, the *duckpools* protocol is composed of three distinct parts: 1) smart contracts, 2) off-chain execution bots, and 3) the graphical user interface or API service. These are further described below.

2.2 Smart Contracts

Protocol smart contracts are open-source and written in ErgoScript. They are immutable pieces of code that enforce the spending rules of the *duckpools* protocol. The key smart contracts of the protocol in its current form, are as follows:

- Pool Contract
- Interest Rate Contract
- Collateral Contract
- Repayment Contract

A simplified scheme of how these contracts interact with each other is shown below:

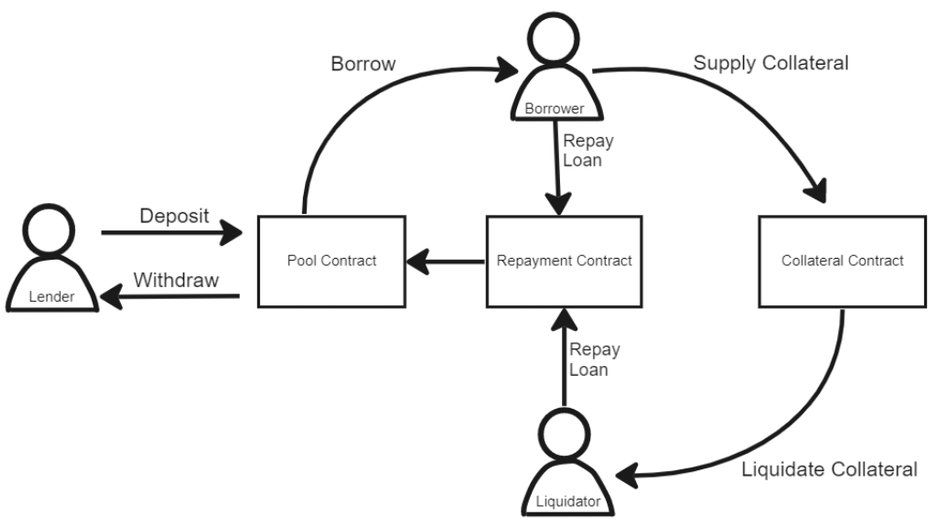

Figure 2: Simplified Contract Interactions

Note that the Interest Rate Contract has not been illustrated in this diagram. This is because the Interest Rate Contract does not interact directly with any part of the protocol; instead, it is used as a data-input (a read-only UTxO) which simply reports the interest rate of a given pool to the involved contracts, calculated using some predefined interest rate algorithm custom to each lending pool.

2.3 Off-Chain Bot Execution

Off-chain execution bots are permissionless bots that execute user orders and liquidations on the platform. They are designed as open-source clients that any community member can run. Our off-chain bots also have access to built-in protocol incentives so that these clients can be run to earn execution rewards.

2.4 User Interface

The user interface is the medium in which borrowers and lenders will commonly experience the protocol. Our team has designed a graphical user interface (GUI), hosted on the domain duckpools.io. To maintain a competitive advantage, the current GUI on duckpools.io is closed-source. However as

described in our *Feature Development Budget* section, a condition of our upcoming token launch is that this GUI will eventually become open-source and community-owned. For the security-orientated user, all transactions through the GUI show the exact transaction to be signed in the browser's developer console, which can be used to verify safety of funds. Otherwise, users can directly interact with the smart contracts through node or explorer calls or some third-party GUI.

3 Tokenomics

We view the *duckpools* protocol as a tool built for the Ergo community. Whilst Initial Coin Offerings (ICOs) and Initial DEX Offerings (IDOs) have demonstrated themselves as innovative and disruptive ways for new cryptocurrency protocols to attain funding, they have often left participants in the rough; with scams and large sell-offs commonplace and many platforms never actually generating sufficient revenue or value to justify the initial fundraising. Furthermore, many token creations have often impeded the functionality or purity of a platform for average users, where features and yield opportunities in financial products are often reserved for token holders only. This creates unfair and convoluted market dynamics. *duckpools* looks to address these shortcomings by offering a fully transparent feature development budget, which explains and justifies all major funding allocations, and by isolating token utility from the platform's function.

3.1 Token Utility

The *duckpools* token, *QUACKS*, offers a simple yet powerful utility to its holders - *governance*. For us *governance* is not just a buzzword to throw around; token holders will have genuine ownership over the protocol's decision-making and finances. *All* platform revenue for *life* shall be directed to the token treasury. Token holders, and token holders alone, hold exclusive voting rights to the usage of treasury funds. Whether token holders decide to simply airdrop revenue to active token holders or use funds to develop new platform features - we, as project founders, will pass on both the responsibility and profits of the *duckpools* protocol, in its entirety, to the community.

Frameworks for a seamless voting and governance experience are described under the *Feature Development Budget* Section.

3.2 Token Distribution

The *duckpools* IDO will be conducted through ErgoPad. A total token supply of 100 million QUACKS will be bootstrapped, with supply allocated as follows:

Allocation Bucket	**Total Supply**	**Percentage of Total Supply**
Treasury	50 000 000	50%
Public Sale Rounds	35 000 000	35%
Team	10 000 000	10%
Liquidity	5 000 000	5%

3.2.1 Public Allocation

Instead of conducting the entire public sale allocations in one release round, *duckpools* will be operating its token sale through three distinct phases. Each phase has differing objectives, however, Phase 1 is designed to fund the early development of the protocol and naturally carries more risk. Later phases are conducted when the platform has already established itself and thus risks are lower for token sale participants. Each phase has its own vesting period and token sale price points. The phase schedule is described below:

Phase	**Vesting Period**	**Maximum Total Supply**	**Token Sale Price ($SigUSD)**
Phase 1 - Early Development (ErgoPad Stakers)	12 Months	3 150 000	0.0135*
Phase 1 - Early Development (Public)	6 Months	3 150 000	0.0190*
Phase 2 - Platform Fruition (Public)	6 Months	20 650 000	Variable**
Phase 3 - Platform Extensions (Public)	3 Months	8 050 000	Variable**

*All proceeds from the token sale shall be converted to SigUSD, if, after this conversion, the proceeds are in excess of the budget's requirements then any excess assets shall be sent to the treasury.

**To ensure the correct level of funding is achieved in phases 2 and 3, Token Sale Price is to be set one week before the token sale. The sale price shall be set to 10% lower than the market value (as given by Spectrum DEX or otherwise the price feed with the highest weekly volume) of the token at this time.

The amount of funding raised in any sale phase shall not exceed the quoted budget in the *Feature Development* Section, unless otherwise agreed upon by active token holders, consequently:

- In Phase 2, all tokens sold to the public shall be sold at their fixed price (calculated 1 week before token sale), however, if it is not necessary to sell the entirety of tokens allocated for phase 2 to reach the funding target, then any surplus tokens shall be allocated to phase 3.
- In Phase 3, all tokens sold to the public shall be sold at their fixed price (calculated 1 week before token sale). However, if it is not necessary to sell the entirety of tokens allocated for phase 3 to reach the funding target, any surplus tokens shall be distributed proportionally among active token holders (team, treasury, and liquidity token holders shall not qualify for this distribution)

All publicly allocated tokens are emitted daily during the vesting phase to token holders. Users can claim emitted tokens through the ErgoPad dashboard at any time. The first emission date shall be one day after the token generation event (the completion of the token sale). Public tokens cannot be used for voting or be eligible for any asset distributions to active token holders until they are emitted.

3.2.2 Treasury

From the moment the *duckpools* IDO is complete, *duckpools* will operate as a decentralized autonomous organization (DAO) and the first decision token holders will have made through their participation in the token sale is to allow the current team to use the generated funding to develop the features detailed in the Budget Section. The development of these features aims to take the protocol far, however, to develop features outside of the Budget's scope or grow the platform in other ways, the treasury can be used. The treasury shall receive the entirety of the platform's revenue for life (this is a condition of the protocol's smart contracts) and as such, it is plausible for the treasury to receive a whole bucket of asset types. Initially, there shall be 50,000,000 *QUACKS* stored under the treasury smart contract, however, over time new assets may accumulate. Since the initial development of the platform mostly relies on funds generated from the token sale, treasury *QUACKS* (and any revenue) will be locked for 6 months from the completion of the Phase 1 token sale. This locking period is needed so that a DAO-structured treasury contract can be built that will support automated decision-making and voting for token holders.

3.2.3 Team

Team tokens are locked and vested for 24 months, emitted daily. The first emission shall be 6 months after the token generation event. Team tokens cannot be used for voting and are not eligible for any asset distributions to active token holders until they are emitted.

3.2.4 Liquidity

A token allocation has been set for bootstrapping liquidity on Spectrum DEX. In Phase 1, 12.5% of the funds raised from the token sale shall be set for

liquidity. The bootstrapped liquidity shall be offered on Spectrum at a price 50% higher than the public token sale price for Phase 1 (rounded to the nearest 0.001 SigUSD) where the number of *QUACKS* needed for this liquidity offering shall be taken from the liquidity allocated tokens.

In Phase 2, 10% of the funds raised from the token sale shall be set for liquidity. The bootstrapped liquidity shall be offered on Spectrum at a price 65% higher than the public token sale price for Phase 1 (rounded to the nearest 0.001 SigUSD) where the number of *QUACKS* needed for this liquidity offering shall be taken from the liquidity allocated tokens.

Any remaining tokens in the liquidity allocation contract shall be sent to the treasury contract after the completion of Phase 1 and Phase 2.

4 Feature Development Budget

The purpose of the *duckpools* IDO is to generate the initial funding to advance the protocol into a market-competitive position and to transition from a private to a community-owned protocol. We have prepared a feature list, compiled by analyzing current market leaders and by gathering feedback from within the Ergo community and wider crypto space, that provides sufficient features, user experience, and frameworks for *duckpools* to be considered a leader in the lending markets. By obtaining fair market quotes for the development of these features we have provided a transparent budget for the usage of token sale funds.

4.1 Phase 1 - Early Development Budget

The main purpose of the Phase 1 token sale is to raise the initial funding to implement upgradeable protocol designs, perform initial security audits and implement some necessary quality-of-life features for borrowers. If successfully funded and developed, Phase 1 shall deliver a protocol that can grow and stand on its own, even if subsequent funding rounds are unsuccessful. As such, we view the Phase 1 budget as the funds needed to reach a minimum viable product. The entire budget for this phase is outlined below:

Feature	Description	Quoted Cost ($USD)
Upgradeable Protocol Design	Establish protocol frameworks that allow for pool upgrades through governance. Frameworks should support the ability to update: • Pool Interest Rate Algorithms • Accepted forms of collateral (and allow for adjustable minimum loan-to-value ratio) • Accepted Price Oracles and DEXs for liquidations • Liquidation thresholds and penalties	15000 - 25000
Interest Rate Contract Longevity	Extend the lifespan of the pool interest rate contract (beta contracts can only survive for about 1 year) to at least 100 years by using multiple interest contracts or smoothing algorithms	3000 - 5500
Security Audit And Bug Bounty	Security audit of all platform smart contracts and their interactions and establish a bug bounty with remaining funds.	5000 - 12000
Treasury Contract Creation	Create a treasury contract that allows token holders to access treasury funds through voting. The treasury contract should have: • Mechanisms in place to control spending (spending cool-downs and allowances) • An adjustable consensus model • Some preset spending paths (e.g. airdrop all token holders some percentage of the treasury) • Capacity to send funds to any Ergo address with pre-defined registers	6000 - 10000
Variable Liquidation Penalty	Allow pools to set custom liquidation penalties (currently, the penalty is set to the maximum which can create a poor borrower experience)	6000 - 10000

Collateral Top Ups and partial repayments	Allow borrowers to add and remove collateral on active loans as well as make partial repayments	5000 - 8000
Front-end Restructuring	Restructure and improve loading efficiency of front-end elements, accounting for implementation of new features	2500 - 3500
Articles, User Guides, and Video Tutorials	Social engagement efforts made through articles, user guides, and video tutorials.	3500
Legal Fees	Cover legal fees relevant to costs of the token sale	4500
Server Fees	9-month allowance for hosted services: • duckpools.io website hosting • Public Ergo Explorer Instance • 3 Off-chain Bots	900
Token Sale Landing Page	Recoup costs involved to build landing page for token sale	1500
Liquidity Provision	12.5% of funds raised to be allocated to liquidity on Spectrum DEX	7557 - 12057
ErgoPad Fees	Fees for conducting launch through ErgoPad	3182 - 5077

Minimum required funding: **$63639**
Maximum required funding: **$101534**

All quotes have been prepared by using quotes from developers, content creators, and legal firms. The token sale conductor can use funding from the token sale at their discretion, however, the cost of each feature should not exceed the amount allocated for its development, unless otherwise amended by active token holders through a community vote. Monthly financial statements shall be prepared that show how and when funds have been used and their corresponding on-chain transaction ID. If the amount allocated for a feature is in surplus of the amount of funds used, then the remaining funds should be sent to the protocol treasury contract.

As can be seen in the quoted cost column of the Phase 1 budget, some features have been ascribed a cost range. Features with a cost range are features that the current team can work on to help reduce development costs. Whilst the maximum of this range is regarded as the fair market quote for the feature, the team can absorb some of this cost if the token sale does not generate sufficient funding. Any unsold tokens from an insufficiently funded token sale will be burnt, which in turn, compensates the team as it increases their relative token ownership (since team token allocation is fixed). With this in mind, all token sale phases will be conducted with the following conditions:

- There is a minimum number of tokens that must be sold (the minimum

funding target)

- If the minimum number of tokens are not sold, then all participants shall be completely refunded for the purchase of their tokens (less network fees)
- There is a maximum number of tokens that can be sold (the maximum funding target)
- If the amount of tokens sold falls between the minimum and maximum number of tokens to be sold, then any unsold tokens must be burnt and the funding allocated for each feature (with cost ranges) in the development plan must be proportionally reduced to align with the reduction of tokens sold.

Whilst there is no formal deadline for the completion of works, a reasonable assessment of the work to be delivered has an estimated completion time of late May 2023. Completion of works later than July 2023 should be regarded as a failure by the token sale conductor. Subsequent token sale phases cannot take place unless all features of Phase 1 have been completed or sufficiently addressed unless otherwise agreed by token holders through a community vote.

4.2 Phase 2 - Platform Fruition Budget

Phase 2 of the *duckpools* IDO is the most feature dense of all the phases, overseeing the implementation of numerous protocol upgrades and quality-of-life improvements, an entire revamp of the duckpools.io user interface, as well as some marketing and branding. The feature development budget is shown below:

Feature	**Description**	**Quoted Cost ($USD)**
Upgradeable Protocol Design	Completed frameworks for adjustable protocol design with an increased emphasis on long-term vision. Pools should be able to undergo major upgrades and support most new features without requiring a protocol hard-fork.	15000 - 25000
Automated Exit Thresholds	Allow borrowers to set an exit threshold on their loans to avoid liquidation penalties using smart contracts and off-chain bots.	11000 - 15000
Pool Dashboard	Dashboards for every pool on duckpools.io. Dashboard should display line graphs of interest rates (borrow and supply), current utilization chart, and key pool information.	6000 - 9000
Mempool Pending States	Implement pending balances on duckpools.io which show user balances inclusive of unconfirmed transactions.	2000 - 3000

Real-time UI updates and continuous yield delivery	Build smart contracts and off-chain bots that continuously deliver yield to lending pools (irrespective of whether a borrower repays their loan) and implement real-time updates to user positions on duckpools.io	20000 - 35000
Compounding Interest Rates	Allow for pools to select either simple or compounding interest rate models and update interest polling rate frequency.	7500 - 12000
UX Design and branding	Engage with UX design and branding agencies to research and tailor a suitable UI design for duckpools.io and its associated branding	15000 - 35000
User Interface Overhaul	Overhaul the entire user interface with respect to UX agency advice.	25000 - 35000
User Dashboard	Dashboard for users which displays their portfolio as a pie chart, history of their transactions, active loans, and positions.	15000 - 18000
Obscure Native Asset Recognition	Update pool contracts to recognize liquidity provider (LP) tokens from external dApps as accepted collateral and lending assets (this extends to duckpools' Lender Tokens).	5000 - 8000
Leveraged Trading Buttons	One-click buttons for leveraged trading facilitated through off-chain bots.	4000 - 7000
Additional Governance Mechanisms	Additional flexibility and structures offered to allow for further consensus reforms or other changes to governance and voting contracts	10000 - 12000
Security	Additional funding for security audits and bug bounties	5000 - 15000
Legal Fees	Additional funding allocation to account for any relevant legal advice costs for subsequent token sales and or changing regulation	5000 - 10000
Social Media	Additional online articles, 1-2 animated videos, social media manager.	5000 - 12000
Servers	Funds to support ongoing server hosting after depletion of phase 1 funds. Aimed to last at least 3 years.	3000 - 5000
Liquidity Provision	10% of funds raised to be allocated to liquidity on Spectrum DEX	17056 - 28444
ErgoPad Fees	Fees for conducting launch through ErgoPad	8977 - 14971

Minimum required funding:	**$179533**
Maximum required funding:	**$299415**

Unlike Phase 1, all features for Phase 2 are ascribed a cost range. For an insufficiently funded Phase 2 the team can absorb the costs for features in which they are involved and the other features will simply have a reduced maximum allocation.

4.3 Phase 3 - Platform Extensions Budget

The primary purpose of the third phase of the *duckpools* IDO is to further fragment community token ownership which will enrich the decentralization of token distribution. By offering a third and final token sale round, *duckpools* will achieve a fairer token launch, with its public allocations spanning a longer time period. Funds raised from Phase 3 shall be used to develop platform extensions. As Phase 3 development is distant, it is difficult to predict desired platform features and fair feature development costs, as such, a concrete development budget for Phase 3 is not yet presented. That said, our current candidate features for Phase 3 are:

- Ability to use lent assets as collateral for loans
- Stable / locked interest rates
- Undercollateralized lending within restricted spending environments
- Fairer governance models

Any selection of the listed features or features outside the candidate list may be included in Phase 3 but the funds allocated for Phase 3 platform development shall not exceed $100,000. A finalized feature development budget for Phase 3 shall be provided before the Phase 2 token sale is conducted.

4.4 Additional Feature Remarks

4.4.1 Governance Guidelines

As described in the *Feature Development Budget*, frameworks for token holder governance shall be contracted out by the *duckpools* team. These frameworks should allow token holders to use treasury funds, issue updates to the user interface, and make any other platform decisions using varied consensus mechanisms. For example, protocol-changing votes should require a supermajority to pass but minor user interface updates may simply require a majority. Furthermore, these frameworks should attempt to restrict treasury spending through spending cool-downs and limits; where token holders can vote to adjust these limits if need be. Ultimately, these voting frameworks should be conservative but also encourage participation and transparency, as well as representing all members of the ecosystem.

4.4.2 An Open-Source GUI

During the development of Phase 2, the *duckpools* user interface and any related code must be made open-source. The website shall be hosted in a decentralized manner on IPFS (or a comparable alternative) and every effort should be made to transfer control of the website to the token holders. The

manager of the duckpools.io domain shall have the responsibility of ensuring that duckpools.io accurately represents token holder decision-making, allowing for any agreed-upon updates to be pushed to the live website. If the manager fails to represent the UI that tokens holders decide on, then we encourage any other parties to host the website in a form that reflects token holder sentiment (which is possible since all the code will be open-source).

5 Closing Statement

The *duckpools* token launch aims to demonstrate the development advantage that the Ergo blockchain has to offer. Through our three-phase token launch, *duckpools* looks to become competitive among the leading lending blockchain protocols for a fraction of the development cost. In total, the *duckpools* token sale fundraising does not exceed $500 000, for comparison, the leading 10 lending protocols (ranked by total value locked) raised an average of $33.7M when they used an ICO to fund protocol development (source: Defi Llama). *duckpools* already offers a working beta of its product and has established clear milestones for the usage of token sale funds. We anticipate that lending on Ergo will form a crucial component of the decentralized finance ecosystem and believe *duckpools* will become the staple lending protocol on Ergo for the future. We envision that *duckpools* will become the flagship example of a well-designed and executed Ergo product.

6 Disclaimer

The *duckpools* token launch will be conducted by an entity that shall remain anonymous. The token launch and its proceeds will be controlled solely by this entity. The creators of the *duckpools* protocol, referred to as the team in this paper, have transferred ownership of any intellectual property regarding the *duckpools* protocol to this entity. The team may or may not be engaged by this entity as contractors for platform works, however, ultimately any revenue generated from the token sale may be used at the discretion of this entity which will hold the private keys over the funds raised. By engaging with the token sale, you accept that the token you are purchasing offers no legal rights to you as a purchaser. If you purchase this token you must do so without any expectations of future returns and must do so in compliance with your local laws. By purchasing this token you must do so with the knowledge that the token is not a financial product (security, derivative, or otherwise) and you understand that there are no obligations offered by the token sale conductor to you as a purchaser, despite any comments made in this paper or elsewhere. The team accepts no responsibility for the sale of this token or any future form the token may take, instead the token conductor is responsible for the token sale. A purchase of the token, *QUACKS*, must be done with no expectations of return (both monetary and obligatory) and thus must be purchased for purely non-monetary reasons. The token sale conductor and the team accepts no liability for any comments or misinformation spread in this paper or elsewhere. The information presented in this paper may be inaccurate and parties engaging with the token sale must also accept this.

References

[1] Ergo Developers, "Ergo: A Resilient Platform For Contractual Money" 2019

[2] duckpools Github, https://github.com/duckpools