Whitepaper

Version 0.1
Q3 2021

Abstract

We are in the midst of a global switch of the fundamental financial train tracks that we use as a global society to trade and transact at the retail and wholesale level, aided by blockchain technology evolution. In this paper, we showcase Indigo Protocol to assist in that transition for the people. For a majority of the world's billions of people, in fact, fair access to the financial tools of this world is all but inaccessible. Accessible for the accredited and wealthy, but not the person in a developing country or without certain credit.

With Indigo Protocol, our mission is to bring the world's financial and equitable assets to the blockchain allowing everyone access to them, in a synthetic form, to control their own financial destiny. As great wealth distribution takes place with money flowing out of the western and developed world and into other countries, Indigo Protocol will be just one tool in decentralized blockchain that will help this long overdue, more free, and fair distribution to happen seamlessly.

Indigo

Table of Contents

Introduction

Meet Blue, an avid investor who has recently become interested in synthetic assets. Blue believes that decentralization and the blockchain are powerful tools. Blue has learned about the Indigo Protocol and wants to begin using it instead of the highly centralized, expensive brokerage accounts.

Violet is a retail day trader located in Nigeria, and she regularly invests in West African, US, Chinese, and other equity markets. Living outside of the countries where the markets trade has a unique set of challenges. For example, trading in the US and Chinese stock markets requires a lengthy AML/KYC process, and the workflow to fund her US and Chinese brokerage accounts as an international trader is grueling.

Both Blue and Violet have cost-saving and accessibility incentives to use the Indigo Protocol. Blue is incentivized by the low cost to mint synthetic assets and the availability of decentralized exchange platforms they may use to trade or supply their tokens as liquidity providers to earn trading fees from other users. Violet is incentivized to trade synthetic assets, called iAssets, built on Indigo since she can trade all of her assets on a single platform around the clock.

What Are Synthetic Assets?

Synthetic assets are cryptocurrency derivatives that resemble traditional derivatives (tracking the price of an underlying asset) but are far more composable, accessible, and verifiable. So, for example, we can lock up some collateral to create a synthetic asset called iXAU that has the same value as gold on the Blockchain without having any real gold in the first place. This gives users exposure to a variety of assets without the need to physically own the underlying asset. These assets can be fiat currencies, commodities, stocks, or anything that has value in the real world. With its transparency, efficiency, low barriers to entry, and decentralized traits, the Blockchain can smoothly deliver all these assets to anyone with access to the Internet.

Synthetic assets can also be used as a lego piece in a wider DeFi ecosystem, helping create and maintain massive markets and applications that rely on them. So, for example, we can create a synthetic asset pegged to the USD that can be used in “fiat” lending protocols.

Market & Users

Synthetic assets can create massive markets thanks to the following properties:

- They can track many different types of assets, basically anything with a real-life value. Hence being able to create many markets for all these assets.
- There are no backed assets or custodians involved to introduce inefficiencies to processes.
- There is a low barrier to entry. Anyone with cryptocurrency can lock some up to mint new synthetic assets, or buy and trade them on the open market.
- They can be used as a lego block in the entire DeFi ecosystem.

Like most DeFi protocols, Indigo needs cash flows to incentivize different actors in the platform. These can be trade fees from DEXs where Indigo users can provide liquidity with their diverse token types. Essentially, Indigo users can mint new synthetic assets to create new markets on different AMMs, and provide liquidity to them for yield farming.

Users can also use synthetic assets directly on other protocols. For example, iUSD can be used as either collateral or loan money on lending applications. In addition, users can use iTSLA and other stock synthetics on stock-specific platforms.

In general, Indigo brings many new assets to the whole DeFi ecosystem and more low-barrier-to-entry services to its users.

How It Works

On the Blockchain, anyone can lock up some crypto collateral to mint new synthetic assets that can be held or traded like any other native token. Autonomous Oracles update the real-world price of these assets to the smart contracts that use them. This sets a market price for trading and calculates the collateral ratio to guarantee that minted synthetic assets are over-collateralized at all times. The protocol liquidates the collateral of under-collateralized synthetic assets to ensure solvency.

The collateral ratio cr at any given time is the ratio of the collateral value over the minted amount value.

$$cr = \frac{p_c * a_c}{p_m * a_m}$$

When cr drops below the minimum threshold, the collateral of under-collateralized synthetic assets is liquidated to ensure solvency.

We're designing an extended version of the Stability Pools that Liquity has introduced. This still allows a low collateral ratio, more automatic and guaranteed liquidation events, but extra efficiency thanks to Cardano's low transaction cost. We also have to adapt to the many more token types in our protocol, but the underlying idea is still there. Users can provide stability by depositing iAsset tokens, which will be used to pay the debt of under-collateralized CDPs in exchange for a share of the claimed collaterals and INDY.

With the minted assets, users can trade to go short, deposit into liquidity pools for yield farming and staying long, or deposit into the stability pool to gain a net profit on liquidation events of other debt positions.

All procedures are transparent, decentralized, and tracked by smart contracts. No one is powerful enough to modify the protocol at will. Like enabling a new kind of asset to mint, all changes must go through democratic on-chain voting processes.

Going Short

Blue thinks that Tesla's stock (TSLA) is overvalued and is going to drop in price. He currently has USD Stablecoin that he uses as collateral to mint iTSLA. Blue immediately trades away his iTSLA. Once the iTSLA price drops, Blue trades back the minted iTSLA at a cheaper price, returns it to get back his collateral at a net profit.

Going Long

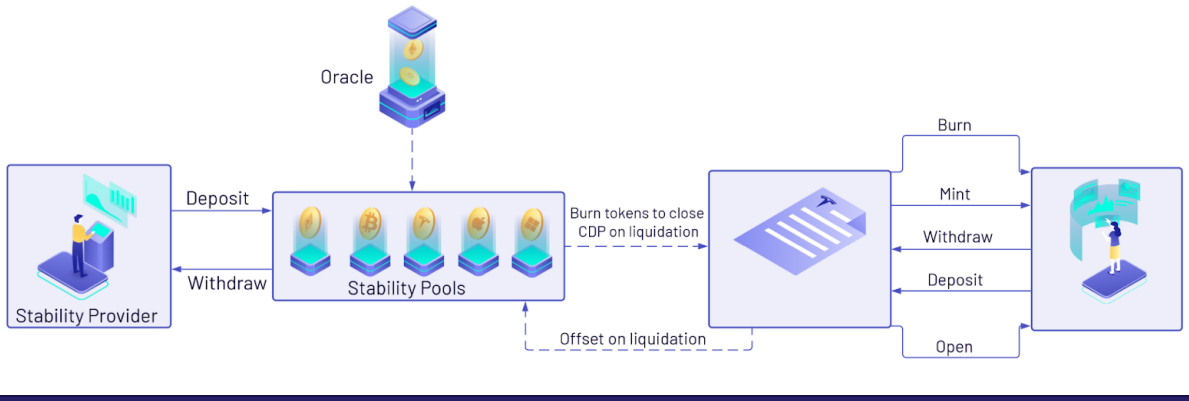
Violet thinks that Tesla's stock (TSLA) is undervalued and is going to rise in price. She trades some USD Stablecoin tokens for iTSLA, then deposits them into a liquidity pool for yield farming. Once the iTSLA price rises enough and Violet wants to cash out, she withdraws her iTSLA with yield from the liquidity pool. She then trades back more USD Stablecoin for a net profit.

Stability Pool Redemption

Blue thinks that iTSLA is going to rise in price and observes many under-collateralized debt positions that minted it. He trades some USD Stablecoin for iTSLA then deposits them into the stability pool. For each liquidation event, Blue's iTSLA is burned to offset the loan, for him to get back a lot more USD than his initial investment, thanks to both the price rise, and the instant net profit on the collateral.

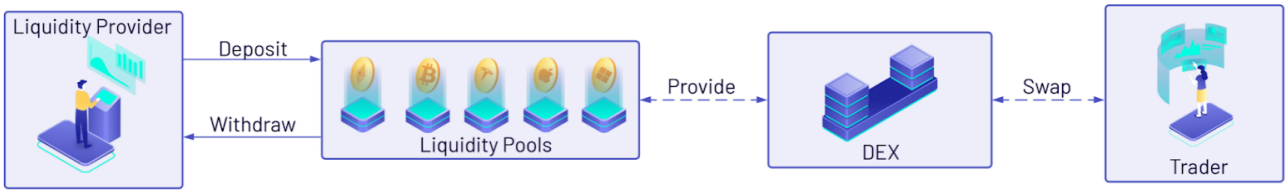
Protocol Overview

The below diagrams show different functionality of the application and how they interact with different users of the Indigo Protocol.



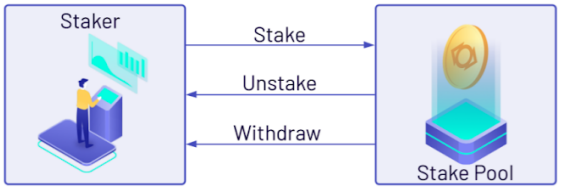
Minting & Stability Pool Functionality

Minting and Stability Pools are key features of the Indigo Protocol. Minting allows any user to open a Collateralized Debt Position in return for an iAsset. Stability Pools are then used to peg the price of the iAsset to the real-world value.



Providing Liquidity to DEXs

By providing both an iAsset and stablecoin, you can pool your token to provide liquidity to the protocol and participate as a liquidity provider.



Staking $INDY

The native asset of the Indigo Protocol, the $INDY token, can be staked to vote on active polls and is required as a deposit for making new governance suggestions.

Smart Contracts

We choose the Cardano Blockchain for its research-first approach. We're not going to bet massive markets on an under-researched blockchain that proves to be insecure or not scalable in the long run. Cardano also provides a great functional programming toolset that improves software correctness and efficient transactions that are inexpensive and fast to execute.

Mint

The Mint contract provides users endpoints to mint new synthetic assets and manages their corresponding collateral deposit positions (CDP). A CDP must maintain a minimal collateral ratio depending on the iAsset that it mints (usually 150%-200%). It will be liquidated if it can't.

Endpoint	Description
Open Position	Deposit some collateral to open a new CDP that mints a chosen iAsset. The iAsset must have been whitelisted. The collateral must be a USD stablecoin or iAsset. And the collateral must satisfy the minted iAsset's minimal collateral ratio.
Deposit	Deposit more collateral (of the same type) to an owned CDP.
Withdraw	Withdraw collateral from an owned CDP. The CDP must still maintain its minimal collateral ratio after the withdrawal.
Mint	Mint more iAsset against an owned CDP. The CDP must still maintain its minimal collateral ratio after the withdrawal.
Burn	Burn some iAsset against an owned CDP. Close the position and return the collateral if all outstanding minted tokens were burned.
Liquidate	Liquidate an under-collateralized CDP. The collateral is sent to the stability pool which repays the debt by burning the outstanding amount of minted iAsset.

Stability Pool

The Stability Pool contract provides endpoints for providers to deposit iAsset and withdraw rewards from liquidated CDPs' collateral.

Endpoint	Description
Deposit	Deposit iAsset as stability, to be burned on liquidation events to pay debt.
Withdraw	Withdraw deposited iAsset or recorded reward from liquidated CDPs' collateral proportionally to the deposited amount. The withdrawal address can also be a CDP.

Oracle

The Oracle contract provides endpoints for oracles to update the new prices of assets as they change in real-time.

Endpoint	Description
Feed Price	Update the price of one or more whitelisted assets. The signer must be the registered oracle of these assets.

Stake

The Staking contract provides users endpoints to stake INDY tokens to receive more INDY tokens as a reward. Protocol users also need to stake to vote on governance proposals.

Endpoint	Description
Stake	Send tokens to the stake pool to stake.
Unstake	Withdraw recorded reward from the stake pool.
Withdraw	Get back the recorded staked tokens from the stake pool.

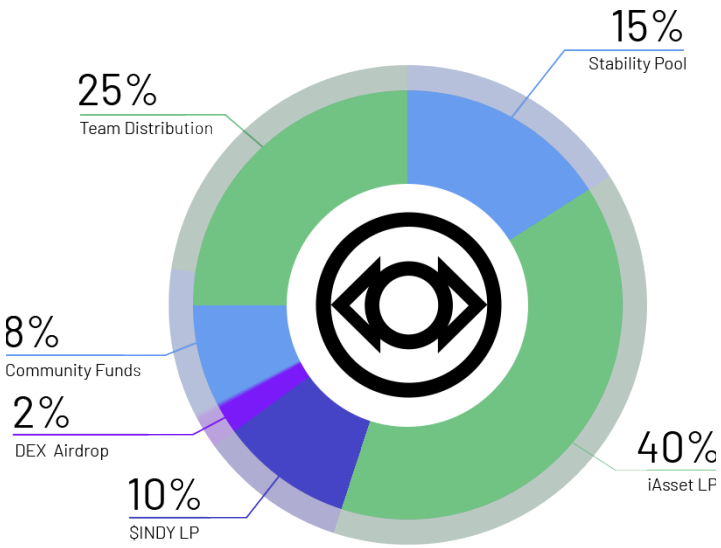
Governance

The Governance contract provides users endpoints to propose changes to the protocol and voting on them.

Endpoint	Description
Open Proposal	Deposit some INDY tokens to open a new executable proposal.
Vote	Vote on an open proposal. The signer must have staked INDY, and not voted already.
Execute	Execute a passed proposal. The current block must exceed the proposal's effective delay.

Vesting

The vesting contract distributes the INDY tokens to different agents based on a predetermined schedule. It exposes no user endpoint for external interaction.



Tokenomics

INDY is the protocol's governance token. It is mainly used for governance but also used as a reward for stakers in the platform. The total supply of INDY is 35M tokens with a 6 decimal precision. We believe in a distribution of the INDY tokens, therefore there will be no pre-sale and private distribution to investors.

The INDY tokens have already been minted, all at once, to be distributed to the community as shown below. And by a monetary policy that disallows future minting and burning.

INDY Token Distribution

Percent-based Distribution Schedule						
	Genesis	Y1	Y2	Y3	Y4	Total Distribution
Stability Pool	15.00%	0.00%	0.00%	0.00%	0.00%	15%
iAsset LP	0.00%	15.00%	12.00%	8.00%	5.00%	40%
INDY LP	0.00%	3.00%	3.00%	3.00%	1.00%	10%
DEX Airdrop via. Governance Vote	0.00%	2.00%	0.00%	0.00%	0.00%	2%
Community Funds/DAO Treasury	5.00%	0.00%	1.00%	1.00%	1.00%	8%
Team Distribution	7.00%	7.00%	6.00%	5.00%	0.00%	25%
Total Supply Distribution	27%	27%	22%	17%	7%	100%
Token Parameters						
Total Supply In Millions	35					

- **Stability Pools:** We reward INDY to stability providers, who deposit iAssets in preparation for guaranteed collateral liquidation. This is critical for both system solvency, user experience, and security against liquidity risks.
- **iAsset LP:** We reward INDY to iAsset LP stakers for their commitment to the iAssets LPs, essential to the whole ecosystem's liquidity. Without them, it's not easy to do useful things with the minted iAssets.
- **INDY LP:** We reward INDY to INDY stakers, who stake to participate in the governance processes of the protocol. We need such incentive for more people to hold INDY, which in turn balances our decentralized system. This prevents having a few whales who run the system.
- **DEX Airdrop:** We need a DEX to expose the iAssets further and create a revenue stream from yield farming for different agents in the protocol. Gifting INDY to DEX users isn't just a nice gesture to be part of a bigger ecosystem; it drives our collaboration with the DEX. The plan is to choose the concrete DEX after a certain amount of time (1 year after genesis) through democratic governance voting.
- **Community Funds:** This is a small pool of funds that can be spent through a governance proposal to fund future contributors and partners of the protocol mainly.
- **Team Distribution:** This is the reward for the initial development team to develop and maintain the protocol until stability is absolute.

INDY Token Staking

The INDY token can be staked to be used in the governance processes. INDY Token holders who have staked their position can vote on polls. Voting power is then weighted by the total amount of staked INDY each holder has. Therefore, users with a larger amount of INDY tokens will have more influence on voting. We have done careful tokenomics distribution to prevent whales in the ecosystem who control it. No presale, with live rewards distributed fairly among different protocol agents.

INDY stakers will be rewarded with more INDY. This doesn't just empower dedicated participants, it incentivizes people who lock it down for governance, for the growth of the whole protocol.

iAsset Tokenomics

iAsset tokens are over-collateralized synthetic tokens that are minted and burnt through the Mint contract. iAsset tokens give users price exposure to real assets, as well as allowing fractional ownership of the underlying asset, with decimal precision of 6. iAssets

cannot be created without collateral, which allows the Indigo Protocol to efficiently peg the price of the token through our state-of-the-art liquidation model.

Monetary Policy

iAsset tokens can only be minted and burned against a CDP through the Mint smart contract. Therefore, their validation rules are tied to the Mint endpoints being called.

Governance

The Indigo protocol is fully decentralized in that no one is powerful enough to change it at will. Instead, all changes must go through a democratic governance process. INDY holders can deposit a small sum of Proposal Deposit to open new proposals for other INDY stakers to vote on.

Initially, INDY holders can start the following proposals:

- White list a new synthetic asset type to make it mintable.
- Delist an asset in the event of unstable market conditions, making it no longer mintable.
- Update protocol parameters, like the minimal amount of INDY tokens required to open a new proposal.
- Spend the community fund for new development, Indigo Improvement Proposals, and Bug Bounties.

After a Voting Period, if the amount of staked INDY participants and the ratio of yes over no votes pass both minimum requirements, the proposal passes. However, the protocol will wait for an Effective Delay before making the change to ensure a smooth transition. For example, upon whitelisting a new iAsset, its oracle might need some time to stabilize.

Protocol Parameters

These are the protocol parameters that can be updated through governance.

Name	Type	Description
Minimum Collateral Ratio	Per iAsset	Each asset might have a very different underlying market, volatility property, and stability pool volume hence needing a different minimum collateral ratio.
Quorum	System	The minimum percentage of stake required to pass a proposal.
Threshold	System	The minimum percentage of yes votes required to pass a proposal.
Voting Period	System	The period (in blocks) in which stakers can vote on a proposal.
Effective Delay	System	The period (in blocks) the system waits before executing a passed proposal.
Expiration Period	System	The period (in blocks) that a proposal has to be executed before being invalidated.
Proposal Deposit	System	The number of INDY tokens need to be deposited to open a new proposal.

Risk Management

We constantly audit the platform and market conditions to inform users with a low collateral ratio that might get liquidated to deposit more collateral. We also provide intuitive tools for the users to monitor and read the market themselves.

We also constantly attack the protocol on both the testnet and mainnet to find vulnerabilities to patch or warn users to avoid risky scenarios if there are any.

For malicious and under-performing risks of oracles and such, we have quick governance solutions to switch oracles or punish bad actors in the platform. This includes falling back to our own Indigo Labs infrastructure, given enough staked votes from the community. We've designed secure incentive formulas for agents to benefit only if they play by the rules, and lose if they don't.

Summary

The activity of trading cryptocurrencies and other real-world assets is steadily spanning beyond the 'professional trader' to the everyday person, globally. The creation of centralized applications like Robinhood & eToro, along with social media figureheads, have driven this exponential rise in interest and investment. Indigo Protocol will satisfy this rapidly growing demand with decentralized synthetic asset exposure for the common person. Indigo protocol will continue to grow significantly in the months and years ahead. Exploring and creating industry partnerships will allow new ideas and concepts to be deployed as blockchain technology and DeFi inevitably grows and evolves as a whole, while enhancements to the protocol will be driven by the user community and governance proposal process. This will ensure that the user community maintains the protocol as the heirs to the platform in true DAO fashion.

References

1. Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, William J. Knottenbelt. (2021). SoK: Decentralized Finance (DeFi). arXiv:2101.08778.
2. Banks, E.. (2015). Synthetic and Structured Assets: A Practical Guide to Investment and Risk. 1-266. 10.1002/9781119206927.
3. Nasdaq. (2021). How Synthetic Assets are Shaping the Future of Crypto Finance.
4. Stanford Liu, Irene Leet. (2021). Mirror Protocol V2.
5. Robert Lauko, Richard Pardoe. (2021). Liquity: Decentralized Borrowing Protocol.
6. Charles Hoskinson. (2017). Why We Are Building Cardano.
7. Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol.
8. Michael Peyton Jones, Roman Kireev. (2020). The Plutus Platform.
9. IOHK. (2020). The Extended UTXO Ledger Model.
10. Dmytro Kondratiuk, Pablo Lamela Seijas, Alexander Nemish, Simon Thompson. (2021). Standardized crypto-loans on the Cardano blockchain.