

dorm dao



Oregon

Presented By: Jordan Brewer



Canto

General Background on Protocol

Canto is an alternative L1 that is focused on free public goods. Its main objective is to support Free Public Infrastructure (FPI). As such, many of the design choices of the protocol reflect this desire to avoid rent extraction and user capture. Rent-seeking refers to an entity looking to increase their wealth without creating benefits to the broader society, and to avoid this Canto minimizes user capture of applications built on the network. It does this by preventing protocols built on the network from having their own front end. Participants go through third party aggregators to avoid user interface-drive ownership, which prevents protocols from charging higher fees from this user capture and facilitates user acquisition for newer protocols. Another important aspect of Canto's aim to provide FPI is to have liquidity as a free public good. There are zero fees for liquidity providers which makes liquidity more accessible by protocols.

Macro Factors Impacting Protocol

Recently Canto has announced it will be migrating to Ethereum as a ZK rollup powered by Polygon Chain Development Kit (CDK). Additionally, it will be focused on bringing Real World Assets (RWAs) onchain. To facilitate this, Canto has partnered with Hashnote and Fortunafi to onboard treasury bills.

Currently the world is in a high interest environment. As we've seen lately, it looks like the rates will remain higher for longer, and this is the predominant narrative going into Q4 2023 as long term bond yields rise. This has tanked crypto prices more broadly as risk free assets increase returns, however protocols that can tap into these increased rates have vast upside. Maker is evidence that protocols that can utilize these higher rates can perform extremely well. On the back of the "higher for longer" narrative, people will be looking for alternative, higher-beta ways to get exposure to this narrative. Canto plays well into the "higher for longer" narrative in addition to ZK layer 2s.

Who's the Team Building the Protocol



X



Canto prides itself on being for the public. For this reason, there are no VC backers, no vesting schedule, no foundation, and no core team of dedicated developers. There was a group of developers that came together to make the chain and received 13% of total token supply, then left it up to the community to build. However, there are several notable players in the ecosystem.

Scott Lewis is a prominent builder and participant in the Canto ecosystem. He serves as the Co-Founder of DeFi Pulse, Slingshot, Hyype, Atrium, and Code4rena, while also taking on the role of Project Lead at Settle. His previous experience includes positions at Susquehanna International Group and Zoo Trading LLC. Additionally, he is a Co-founder of Concourse Open Community, contributing to the establishment of Concourse Constructions, which encompasses Settle Finance, ConcourseQ, Dapped.io, and Layr2.

Another group working on Canto is a development team called Plex. They are chain-native builders with backgrounds in quant trading, mechanism design, engineering, and product. NeoBase is also a team in the Canto ecosystem that does Canto chain analytics, has an RPC endpoint, and makes APIs.

Lastly, Canto governance proposal 43 enables Contract Secured Revenue (CSR). This allows developers to get a percentage of all gas fees generated by their smart contract in perpetuity. This further incentivizes building on Canto.

General Auditing Background for Protocol

Canto has undergone multiple open audit contests by Code4rena (C4) (**Figure 3**). In these C4 open audit contests, participants called Wardens review, audit, or analyze smart contract logic for a bounty. Its first audit was in June 2022 where 63 Wardens participated to find 26 unique vulnerabilities. One week later, they had a second C4 open audit contest that found 14 unique vulnerabilities. Canto's third audit followed shortly after the second in July of 2022. The third audit was a solo audit performed by ghouL.sol that found 4 vulnerabilities, however this audit was performed on a different subset of code. GhouL.sol is a senior solidity developer who serves as a judge for C4 audit contests. Additionally, the Gravity Bridge was audited by C4. More recently, C4 audited Canto's verRWA code which found 11 unique vulnerabilities.



X



Canto code did have a considerable amount of vulnerabilities as of July 2022. Looking at other protocols audited by C4 such as zkSync, EigenLayer, Arbitrum Foundation, and Base, these audits found 6, 4, 6, and 0 unique vulnerabilities respectively. While the scope on all of these audits varies in regards to the number of lines of code, some of them are larger and some are smaller than Canto's audits, and still had considerably less vulnerabilities. The smart contract risk of Canto is a concern going forward, but it is possible that Canto's rebrand to an L2 and utilization of Polygon's CDK could garner more attention by devs to build safe code as well as Polygon to make sure Canto is being helped where necessary. This is something to pay attention to moving forward.

Specific on What Protocol Does

Canto aims to be a free and public L2 on Ethereum. The core functions of Canto are currently its DEX, Canto Lending Market (CLM), and soft-pegged stablecoin \$NOTE. As previously mentioned, the goal of the DEX is to prevent rent seeking so there is no official interface and it runs in perpetuity without a fee switch. It offers two types of liquidity pools: the standard $x * y = k$ and concentrated liquidity pools for deep stablecoin liquidity that use the function $yx^3 + xy^3 = k$.

The CLM is controlled by stakers and is an adaptation of Compound V2. It uses group liquidity for efficiency to avoid the peer-to-peer hassle of matching a lender and a borrower, but this requires liquidity mining incentives to increase lending liquidity. Additionally, the CLM allows LP tokens to be borrowed against (but not lent out).

\$NOTE is the Canto ecosystem's unit of account. It is a fully collateralized soft-pegged stable coin that uses an algorithm to adjust interest rates every 6 hours, pressuring \$NOTE back to a price of \$1. For example, if \$NOTE is trading at \$1.03, lowering interest rates paid on borrowing \$NOTE will incentivize people to borrow which will increase the supply of \$NOTE and decrease the price. Interest rate adjustments are playing on the efficient market hypothesis and arbitrage. All interest paid is held in a community treasury used for public goods funding. For users wanting to borrow \$NOTE against another stablecoin such as \$USDC, this \$USDC can be lent out again from the CLM. The \$USDC borrower will deposit some other form of collateral allowing them to borrow the \$USDC. This allows the \$NOTE borrower to receive the interest payments paid by the \$USDC borrower. Users can deposit \$NOTE into the



X



CLM to get \$cNOTE, which is basically a lending receipt. Users will get yield on their \$cNOTE related to the CLM.

Recently Canto has also made some key partnerships to build out the ecosystem and target RWAs. To name a few, Canto Identity Protocol has partnered with Blank Rasa in creating its identity NFT. The NFT allows users to attach onchain traits like a namespace, profile picture, and bio. Fortunafi and Hashnote have been onboarded to the Canto network to bring RWAs onchain. Fortunafi brings liquidity solutions to stablecoin issuers while Hashnote targets institutional DeFi. RWAs combined with Canto's FPI makes it the perfect environment to build financial instruments on top of tokenized treasuries. These partnerships can already be seen in Canto with US Yield Coin as an RWA to lend to in the CLM. However, since \$cNOTE and US Yield Coin are new, they are not being picked up in DefiLlama, which is important because this further indicates Canto's potential and fundamentals are not accurately priced in. The importance of USYC is that it is a tokenized treasury that full KYC and whitelisted individuals can mint and borrow against, up to a collateral factor of 0.99. With the borrow rate being 1% and the yield on USYC being ~5%, these parties can do a carry trade. Canto's dynamic interest rate will moderate the peg of \$NOTE to make sure people pay back their debt. What this means is that if USYC is yielding the risk free rate of 5%, we would expect the borrow rate to be something like 4.75%, which is what retail traders will get for lending their \$NOTE. Tokenized treasuries is a narrative that has a lot of potential. Additionally, both \$cNOTE and USYC are new assets and as a result, their TVLs are not being updated on DeFiLlama. This is another instance of information asymmetry and evidence that \$CANTO needs to be repriced.

Why the Protocol Offering Matters to Consumers

Building financial instruments and protocols on top of RWAs in an open source manner is a unique capability of blockchain. Canto capitalizes on this by making these instruments secure and accessible by using an easily accessible Ethereum L2 and by focusing on free public infrastructure. As a retail investor owning treasury bills or a treasury bill ETF, there isn't much to do outside of owning it. By bringing these onchain, it opens the door to a vast array of use cases. Additionally, this will give other countries easy access to the US financial system. In second and third world countries where inflation is a big problem, many citizens look to hold their wealth in US currency and financial instruments. Especially in the narrative that interest rates in the US and across the world will remain higher for longer, protocols focusing on



x



onchain treasuries have an opportunity to capitalize on this environment and pave the way towards bringing more RWAs onchain. Not many chains are offering tokenized treasuries right now, which puts Canto in a unique position. Its RWA-backed stablecoin is also an important product to consumers, as seen by \$DAI.

Protocol Versus Competitors Chart

Project	Network	Composable Execution Environment	Core Functions
Canto	Ethereum L2	Yes	<ul style="list-style-type: none"> - DEX - Stablecoin - Lending market - RWA partnerships - Free Public Infra
Centrifuge	Polkadot	Yes	<ul style="list-style-type: none"> - Secure RWAs onchain as NFTs - Executive summary on debts - Investment pools - Maker partnership
Goldfinch	Ethereum	No	<ul style="list-style-type: none"> - Yield from offchain companies - Private credit market
Credix	Solana	No	<ul style="list-style-type: none"> - Credit market
Clearpool	Ethereum, Polygon, Polygon zkEVM	No	<ul style="list-style-type: none"> - Credit market
TrueFi	Ethereum, Optimism	No	<ul style="list-style-type: none"> - Credit market
MakerDAO	Ethereum (soon NewChain)	Yes	<ul style="list-style-type: none"> - Stablecoin partially collateralized by RWAs



X



Frax	16 chains	No	<ul style="list-style-type: none"> - Stablecoin - LSD - Frax Price Index - Collateralization using RWAs
------	-----------	----	---

Many projects in the RWA space focus on being a private credit market, making loans to real world companies earning yield that is uncorrelated with crypto markets. These projects give the ability to invest in different forms of RWAs, however Canto differentiates itself in one key way.

Being an L2 on Ethereum, not only will Canto benefit from the network effects of Ethereum while maintaining cheap and fast transactions, it will also have its own execution environment. Allowing builders to utilize the functionality of existing protocols as free public goods lends itself to create what are known as “hyperstructures”. Canto will be one of the only projects building its own network on top of Ethereum. Along with its focus on infrastructure to use and build on and its partnerships with “the suits” such as Fortunafi and Hashnote, Canto has uniquely positioned itself to capture a large market share in the RWA space.

Protocol Go To Market Strategy Versus Competitors

Canto’s main competitors in the RWA space are Maker and Frax. MakerDAO’s DAI and sDAI have been proven to stand the test of time. However, Maker is a protocol that has some RWA integration through sDAI. While it is a major player in the tokenized treasuries space, it is not a layer 2 network dedicated to bringing all types of RWAs onchain and building financial instruments and infrastructure on top of them.

Frax is another protocol, rather than an L2. Frax offers a hybrid (collateralized and algorithmic) stablecoin, an eth LSD, and Frax Price Index (pegged to a basket of goods). The sFRAX staking yield is intended to track the risk free rate of assets by changing its stablecoin collateral to treasury bills. While this is a form of bringing real world yield onchain, it is not the same function as buying a treasury bill. It is not the same as depositing stablecoin collateral to earn the risk free rate on that collateral, or build financial instruments on top of it.



x



OpenTrade is another blockchain company looking to bring treasuries onchain, however they are not targeting the same audience and functionality as Canto. OpenTrade is looking towards institutional clientele for a suite of b2b functions such as supply chain management.

Many projects such as Goldfinch, Credix, Clearpool, and TrueFi aim to be private credit markets. While this is one way to integrate RWAs, it is not the same approach that Canto is targeting by bringing these assets onchain to be built on and used for capital efficiency.

Other points of comparison include other Alt L1s and L2s on Ethereum.

How Token Extracts Value

\$CANTO extracts value primarily by being the governance token of the network. It is currently used to pay transaction fees on the Canto Network, as it is an L1. However, the investing frame of this report is for Canto as an L2 using \$ETH for gas fees.

By staking \$CANTO, participants can govern the CLM, DEX, and network itself. The governance execution is similar to Compound V2. This control over the protocol and network is what will generate buy pressure on the \$CANTO token. The \$MKR token governs the Maker stablecoin protocol, and it has clearly benefited from the increased use of DAI and sDAI. Canto governance also determines what public goods the treasury will fund.

Additionally, when compared to other L2s and L1s where tokens are used for governance, it is clear that there is demand to hold these tokens. When a network does well, the token typically appreciates in price as well. As Canto brings RWAs onchain through a zk rollup, TVL and network use will continue to grow.

Tokenomics/Vesting Schedule

Since there is no VC backing for Canto, there is no vesting schedule. There is a maximum supply of 1 billion tokens with the following breakdown:

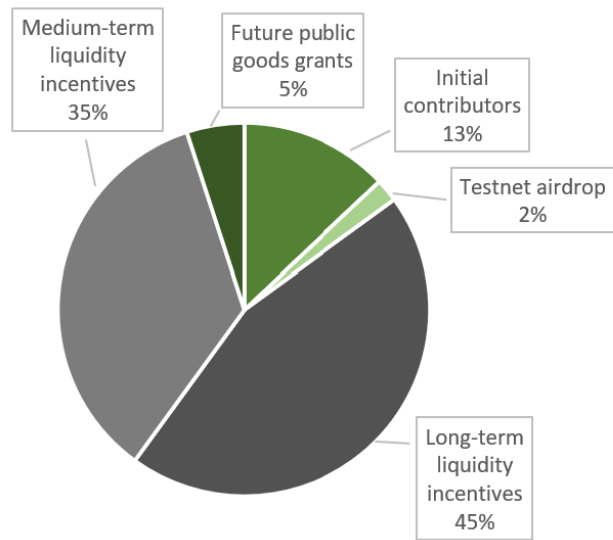
- 13% for initial contributors



X



- 2% for testnet airdrop
- 45% for long-term liquidity incentives (5-10 years)
- 35% for medium-term liquidity incentives (upcoming months and years)
- 5% for future public goods grants



For the first month, \$CANTO inflated at 19.8% APR but for following periods governance will adjust emissions. The docs state that over time, the inflation rate should tend to zero. I could not find any data on current Canto inflation, which leads me to believe it is quite high. Given the current APYs to LP, this appears to be the case.

Modeling/Ratio Analysis

The first lens to look at Canto from is comparing it to other L1s as a metric of FDV/TVL. This comparison indicates that as an Ethereum competitor (alt L1), Canto is undervalued relative to others. The market has valued other alt L1s using a

L1 Network	TVL	FDV	FDV/TVL	WTD Ratio
Canto	54	244	4.52	
Avalanche	486	6,603	13.59	1.95
Fantom	46	586	12.74	0.17
Cardano	152	11,014	72.46	3.25
Algorand	43	885	20.58	0.26
Binance Smart Chain	2,661	42,164	15.85	12.45
Weighted Average				18.08

a much higher FDV/TVL multiple than it does for Canto. This suggests that as Canto continues to get built out as an ecosystem, a much higher multiple could be expected. Using the weighted average ratio of this metric would put Canto at a \$976 million valuation, which is 4 times higher than its current valuation. However, since Canto will be a zk rollup on Ethereum, it is more appropriate to compare Canto to other L2s on Ethereum.



X



When comparing Canto to other L2s through the same lens of FDV/TVL, Canto still appears to be undervalued but not by much. Ignoring the outliers of Mantle and ImmutableX paints the picture that Canto is valued on the low end, but not necessarily undervalued. When comparing Canto to other L2s, two things to consider are the FDV/TVL multiple and the potential TVL. The FDV/TVL multiple is currently reasonable for Canto. However, using this same multiple, what is the implied valuation if the TVL is higher?

L2 Network	TVL	FDV	FDV/TVL	WTD Ratio
Canto	54	244	4.52	0.10
Arbitrum	1,682	8,024	4.77	3.42
Optimism	589	5,198	8.83	2.21
Metis	23	115	5.00	0.05
ImmutableX	34	1,041	30.62	outlier
Mantle	44	2,052	46.90	outlier
Base	302	-	-	-
zkSync	117	-	-	-
Starknet	37	-	-	-
Polygon zkEVM	19	-	-	-
L2 WTD Avg				5.78

Using Canto's current FDV/TVL multiple with a different possible TVLs on the L2 give an idea of what Canto will be valued at. Now looking at the second part of the equation mentioned earlier, what is the expected TVL on Canto? Is it fair to say that Canto has positioned itself to capture a large TVL? I

Potential TVL of Canto	FDV (current Canto multiple)	Percent Increase	Implied Price	Current Price
117	529	217	\$ 0.52	\$ 0.24
302	1,365	559	\$ 1.34	
589	2,661	1,091	\$ 2.62	

I believe this is a fair assumption. As a zk rollup, Canto has positioned itself to capture a large market share compared to being an optimistic rollup. Canto is playing the long game. When focusing on free public goods and RWAs onchain, it is even more likely that Canto will attract a large user base. Canto's partnerships with Fortunafi and Hashnote along with its use of Polygon's CDK leads me to believe that it will attract a TVL that is at least as large as zkSync's at \$117 million. Looking at how fast Base's TVL got to \$302 million, it is reasonable that Canto can gain similar traction and experience similar growth. With a TVL the same as Base's and a conservative FDV/TVL multiple, Canto's token price is \$1.34, a 559% increase from its current price at \$0.24.

A final industry outlook for RWAs is in its projected growth. Boston Consulting Group expects the tokenization of global illiquid assets to be a \$16 trillion industry by the end of the decade, with only \$600 billion in tokenized

Tokenized RWAs 2023	600,000,000,000
Tokenized RWAs 2030	16,000,000,000,000
Years	7
CAGR	59.85%



X



treasuries in 2023. This gives a Compound Annual Growth Rate (CAGR) of 59.85%. This annual growth rate gives more merit to the claim that Canto will quickly attract a high TVL. When comparing this to other industries, this is very high, as most industries tend to have a CAGR between 8%-25%.

Overall, the narrative behind Canto is a powerful one. RWAs as a zk rollup on the back of EIP-4844 with blob space integration is the perfect storm of narratives to have big impacts on price action.

Road Map

There is no core Canto team so an official roadmap does not exist. In a recent interview, Scott Lewis said that Canto is currently doing hackathon style building competitions, and this combined with CSR has been working well for building out the network. He also said he'd like to see a more robust governance system rather than everyone voting on everything. However, with no official team and governance proposals being the main source of direction in the ecosystem, these could change.

Recent partnerships with Fortunafi, Hashnote, Polygon zk CDK, and Blank Rasa suggest that for the short-medium term, Canto will continue building out protocolized RWAs on a zero-knowledge rollup while also integrating onchain identities.

Investment Thesis

Looking to RWAs as a potential catalyst for the next bull market and the next big use case of blockchain technology, Canto positions itself at the forefront of this frontier. Emphasizing free public infrastructure on an Ethereum L2 will lower the barriers to entry to the ecosystem as applications continue to be built. Looking at the recent performance of \$MKR in a high interest rate environment suggests there is demand for tokenized treasuries and financial instruments built on top of them. Overall, \$CANTO needs repricing. It needs to be repriced as an Ethereum L2 and as a hub for RWAs. It needs repricing for its new assets \$cNOTE and USYC, and the TVL for both of these are not yet being picked up by DeFiLlama, creating an information asymmetry in the market and opportunity for returns.



X



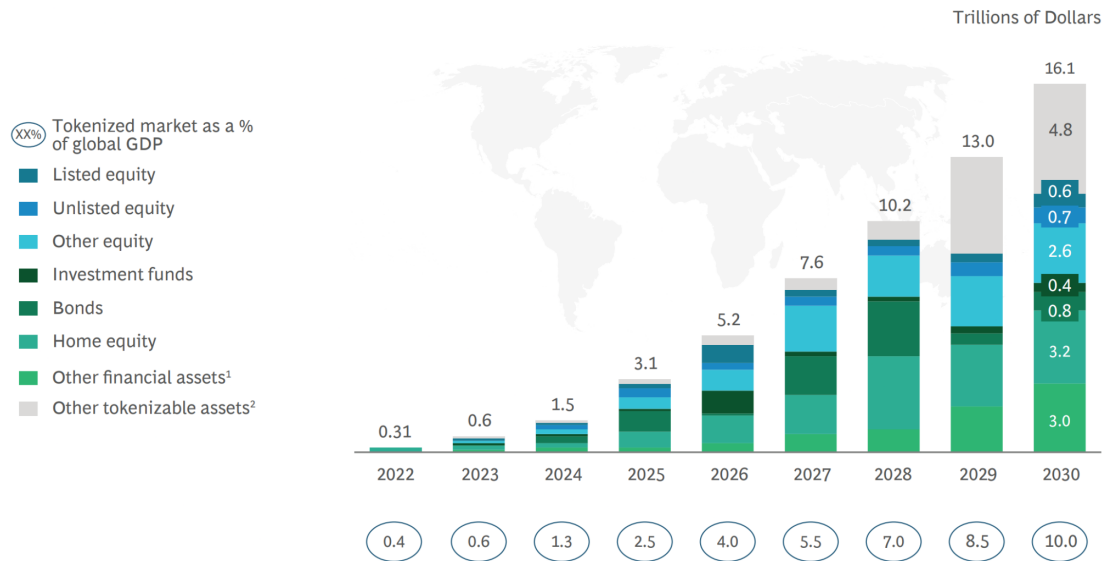


Fund Recommendation

3 ETH

Appendix:

Figure 1: Boston Consulting Group



X





Figure 2: \$cNOTE & USYC TVL Information Asymmetry

ambient @ambient_finance · Oct 16

1/ Introducing Ambient Finance on @CantoPublic – starting with an incentivized liquidity pool for \$cNOTE/USDC.

This Canto deployment of the Ambient DEX brings gas-efficient, highly-customizable trading, which will be used in support of Canto's neofinance infrastructure.



8 37 132 22.9K

Some accounts you follow often like this account

Oxngmi @0xngmi

do you have a list of pools we can use to list this on defillama? doesnt seem like you have a subgraph on canto

10:40 AM · Oct 19, 2023 · 735 Views










Figure 3: Audit Reports



X



Audit Reports

Sort By:	Date Range:	Search:
Report date (Newest first) ▾	All time ▾	🔍 Canto
 Canto → 7 Aug 2023 - 10 Aug 2023	 Canto → 20 Jun 2023 - 23 Jun 2023	 Canto Identity Subprotocols → 17 Mar 2023 - 20 Mar 2023
📄 2023-10-11 View report	📄 2023-09-29 View report	📄 2023-05-09 View report
 Canto Identity Protocol → 31 Jan 2023 - 3 Feb 2023	 Canto → 23 Nov 2022 - 28 Nov 2022	 Canto → 7 Sep 2022 - 8 Sep 2022
📄 2023-04-06 View report	📄 2023-03-31 View report	📄 2023-03-31 View report
 Canto → 28 Jun 2022 - 2 Jul 2022	 Canto → 14 Jun 2022 - 21 Jun 2022	 Canto → 8 Jul 2022 - 10 Jul 2022
📄 2022-10-18 View report	📄 2022-10-18 View report	📄 2022-07-10 View report

Sources:

<https://makerburn.com/#/rundown>

<https://defillama.com/>

<https://www.coingecko.com/>

<https://cointelegraph.com/news/token-adoption-real-world-assets-blockchain>

<https://docs.canto.io/>

<https://canto.io/>

<https://analytics.neobase.one/markets>



X



<https://www.youtube.com/watch?v=vba3Fdx1960&t=3701s>

<https://twitter.com/CantoPublic>

<https://www.missiondefi.com/canto-scott-lewis/>

<https://coinmarketcap.com/community/articles/64be29a20ae92b4c2e42aed1/>

<https://youtu.be/4bWCCY2sGqM?si=JxsP85BsO5nYRVJ1>

<https://youtu.be/4agcJjmcQsw?si=SVkFSRJ8492qroJG>

<https://docs.frax.finance>

<https://app.frax.finance>

<https://www.datawallet.com/crypto/frax-finance-explained#:~:text=Summary%3A%20Frax%20Finance%20is%20a,price%20stability%20and%20user%20governance.>

<https://web-assets.bcg.com/1e/a2/5b5f2b7e42dfad2cb3113a291222/on-chain-asset-tokenization.pdf>

<https://www.zippia.com/answers/what-is-a-good-cagr-for-an-industry/#:~:text=A%20good%20CAGR%20for%20an%20industry%20is%208%25%20to%2012,growth%20rate%20over%20multiple%20years>

<https://x.com/0xngmi/status/1715060426298261555?s=20>

https://youtu.be/gQnusL2eAzA?si=0Mzn0BTE_fQYu70Q

<https://code4rena.com/reports>



X

