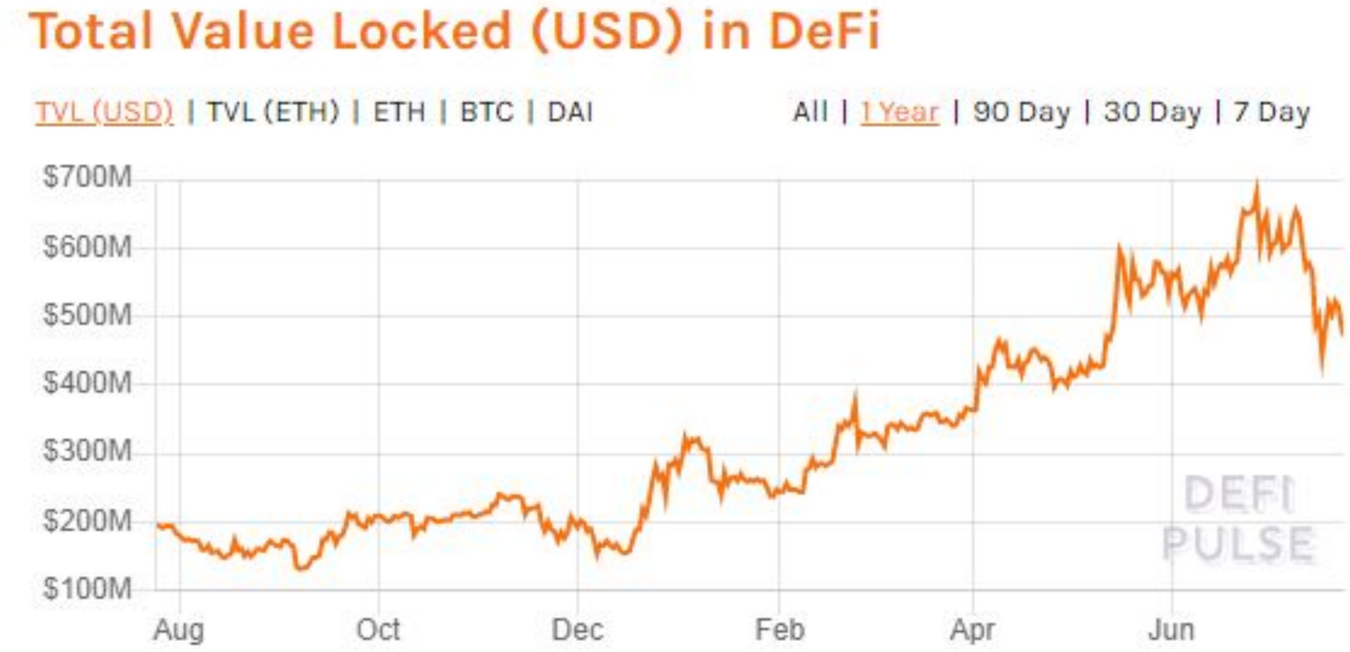
zkCompoundify

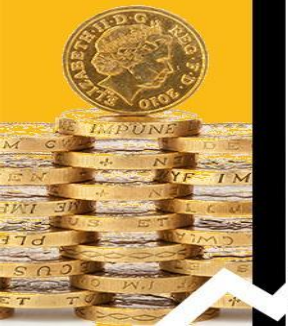
Zero-Knowledge Lending with Compound Protocol

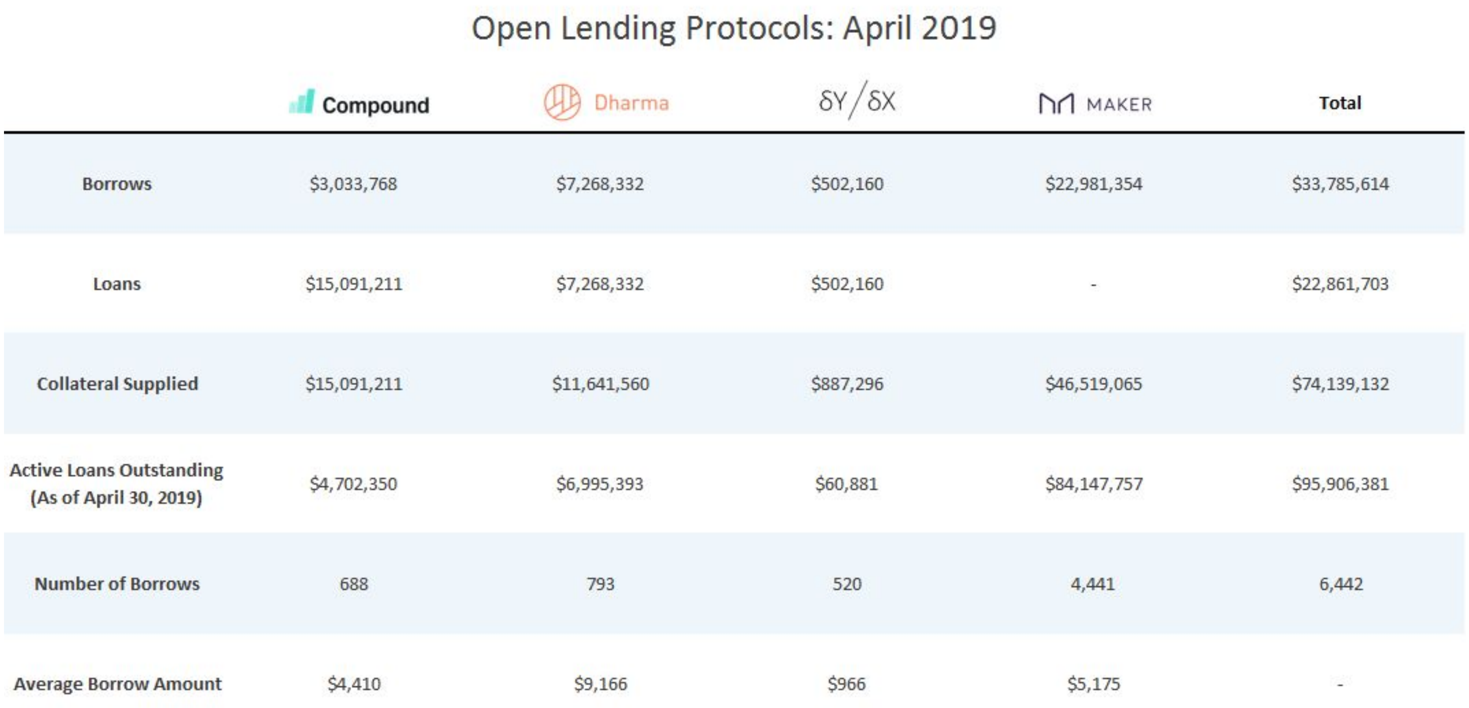
-Tezan Sahu

Booming DeFi



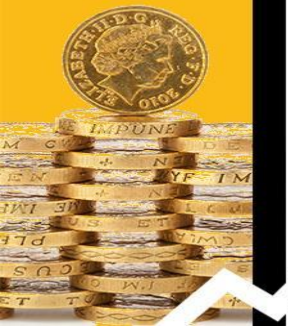
Total Value Locked (USD) in DeFi





Open Lending Protocols: April 2019

	Compound	Dharma	δY/δX	MAKER	Total
Borrows	$3,033,768	$7,268,332	$502,160	$22,981,354	$33,785,614
Loans	$15,091,211	$7,268,332	$502,160	-	$22,861,703
Collateral Supplied	$15,091,211	$11,641,560	$887,296	$46,519,065	$74,139,132
Active Loans Outstanding (As of April 30, 2019)	$4,702,350	$6,995,393	$60,881	$84,147,757	$95,906,381
Number of Borrows	688	793	520	4,441	6,442
Average Borrow Amount	$4,410	$9,166	$966	$5,175	-



Off late, Compound Protocol has been performing very well

The Problem

With great transparency comes bad privacy!

- Stan Lee (Multiverse)

Our Solution

zkCompoundify

Zero-Knowledge loans on Ethereum by integrating AZTEC with the Compound Finance Protocol, and deployed on Matic Network.

Compound Finance Protocol

“Liquidity pool” — you supply liquidity to a market, and users borrow from that market

No Order Matching - Independence of lenders from borrowers

No pre-defined durations or terms

Interest rates are determined algorithmically

AZTEC Protocol

An efficient zero-knowledge privacy protocol.

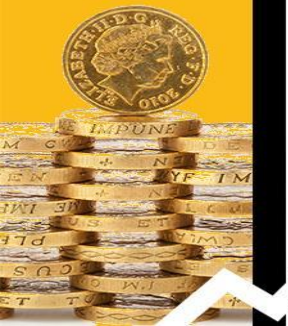
AZTEC powers real world financial applications on Ethereum mainnet today.

Why Matic ?

Low transaction Cost

High transaction throughput

Fastest finality



What we have achieved

A privacy-centric lending protocol, where the loan amount or the borrow amount remains confidential.

Without even knowing the amount, everyone can verify that a transaction is valid.

We have an enormous Business Application in the Enterprise Sector, that has been earlier afraid to use Lending on Blockchain due to its public nature.

Workflow of the Platform

Currently for the PoC, we have demonstrated the lending/borrowing of only DAI & cDAI. This can be well extended to add any number of tokens

1. When the Lender comes to the platform, he may already have DAI or he could convert some **ETH -> DAI** on our platform

2. This DAI is converted into equivalent notes of **zkDAI** (zero-knowledge counterpart of DAI), which would be used for lending. *[These notes have unique NoteHashes & their value can be viewed only by the owner of the Viewing Key, ie, the Lender.]*

3. Now, these notes of zkDAI could be **lent into a Liquidity Pool** in exchange for **zkCDAI** (zero-knowledge counterpart of Compound DAI)

4. These zkCDAI could be used very similar to cDAI & can be **redeemed later** at a higher exchange rate for zkDAI.

Similar but opposite process is followed for Borrowing.

Analysis of the Project

- Currently, the entry/exit points of converting DAI->zkDAI & vice-versa are the only points that could potentially leak information about the maximum amount a person can lend. This could be solved by integrating mixers like Tornado.cash to anonymize the lenders.

- This project would become more successful when zkERC20's would become mainstream such that the zkCDAI obtained by the lender could be spent directly for other productive applications along with just gaining interest.

- With the blazing fast & cost-effective transactions enabled by Matic, large volume lending/borrowing can be conducted seamlessly.

Contract Addresses on Matic Network

- **AZTEC:**
  - **ACE:** 0xc53f83D6485605736C8d4C22095b8725A474ED37
  - **JoinSplit Verifier:** 0x68a6Cec8bbC3E32C22A1EedDbA2B99a230A93B13

- **Tokens:**
  - **DAI:** 0x132077fbcBeBA99A2eEC1E7C006eEb007Fa482Ce
  - **cDAI:** 0x675D00a79E5506B42a0EF09A894064F505C5731d
  - **zkERC20:** 0x0b2f0D7FaA6f35169816d39177379222b3Ed0704

- **CompoundDAIMarket:** 0x031D914c6d145F8ef24E040A1B2EFE5c4e75c92D

Road Ahead...

- Currently the project supports simple Lending/Borrowing. In the future, we could include advanced features that already exist in Compound Protocol and introduce zero-knowledge into it.
- Add more zkERC20 <-> zkCERC20 token pairs into the platform
- Integrate exchanges like Kyber (once they support zkERC20 tokens) to allow users to exchange their zkAssets seamlessly.

THANK YOU!