Credit Rating
Enforcing trust through code

Filippo Caprioglio, Unexployed, N0madCapital

3six9 Innovatio, Cognito Research.
{filooxx, unexployed, n0mad}@3six9.io

October 17th, 2022.

Abstract. The majority of credit rating in the TradFi world is conducted by an elite of entities who use international standards (*FICO, Z-Score*) to rate borrowers creditworthiness. In the DeFi world a whole different approach is required to have enhancements on the handling of huge datasets, privacy protections and pseudonymity maintenance. These hardening requirements command the exploration of solutions including third-party risk assessment, non-fungible credit scores *(NFCs*), machine learning (*ML*), proprietary oracles and blockchains, and zkKYC. Given the importance of privacy and operational security of the DeFi industry, both data encryption and zkKYC are the most developed and implemented solutions with tens of protocols relying on the credit rating and scoring offered by Credora Inc. In this paper, we evaluate new frontiers for credit rating, i.e. performing privacy-preserving credit risk scoring while maintaining decentralization and the access to data. We describe how the lending and borrowing industry can benefit from these innovative approaches and — most importantly — enhance capital efficiency within the space.

Keywords: Credit Rating · Data Privacy · Loan Activity · Machine Learning

Table of contents

Please note: throughout this paper we refer to the industry we operate in as DeFi. We believe that a better representation of this would be better named OpFi but we decided to keep the commonly used term for clarity.

Introduction

A key requirement for undercollateralized lending is credit rating. The reason is very simple: counterparties do not want to lend capital out to individuals who will walk away with the money or to people who have a history of questionable financial behavior. The sole purpose of credit rating and credit rating agencies is to gather enough information to affirm "this user is eligible for this type of loan". Traditionally, credit rating is based on credit scoring, which estimates the risks of lending using elements of quantitative and qualitative analysis.

In the previous paper, "*Undercollateralized Loans*", we outlined the current market landscape regarding this type of service within DeFi. We concluded that without some sort of native form of DeFi credit rating undercollateralized loans are simply not feasible. There needs to be some insurance that the borrower is able to pay back the loan and traditionally that is done through know-your-customer practices (*KYC*). In DeFi, where pseudo-anonymity and privacy rule, there are certain problems with properly conducting KYC. In this paper, we would like to revisit the problems of credit rating in DeFi and solutions currently on the market.

Let's first consider how credit rating is done in the traditional world to offer some context and perspective. In the status quo, the credit rating industry is extremely concentrated. Ninety-five percent of all credit rating businesses are conducted by just three companies referred to as "*The Big Three*". The two firms *Moody's Investors Service* (Moody's) and *Standard & Poor's* (S&P) collectively control over 80% of the global market and *Fitch Ratings* (Fitch) controls 15%. The reason for the high concentration of this market is disputed, with some arguing that it has to do with reputation and that these firms are considered authorities in that regard. This has historically represented a high entry barrier for newer firms.

Credit rating is important as it plays a crucial role in the creation of more liquid markets and forms trust between lenders and borrowers. By assessing the risks involved and the creditworthiness of the borrowing party, the credit rating agency functions as an information intermediary that can be trusted by both parties. Usually, a score is assigned based on an analysis of a person's/entity's credit and often translated to a *FICO standard*.

Earlier this year, DeFi protocol Compound was rated by one of "*The Big Three*", S&P. The fact that a DeFi protocol was being rated by a major, well-respected financial rating agency, was truly a breakthrough and moment of recognition for DeFi. That being said, the rate Compound received was a B-, traditionally interpreted as "junk" and used for distressed, high-yield debt. This score was justified by the skepticism from the TradFi world towards stablecoins, in particular for their "unpeg risks", the high-interest rate offered (≈ 4%), and the incompatibility of stablecoins with fiat money.

Scoring through the Altman’s Z-Score Model

The Altman’s Z-Score model is a formula used in TradFi for determining whether a company is headed for bankruptcy or it may be solvent. The model is numerical measurement used to predict the chances of a business going bankrupt in the next two years.

Z-Score was first developed in 1968 as a measure of the financial stability of companies and combines five financial ratios to predict the probability of a company becoming insolvent in the next two years. The model takes advantage of five financial ratios and the info contained in the $10 - K$ report (*SEC*).

The formula used to compute the score is as follows:

$$\zeta = 1.2T1 + 1.4T2 + 3.3T3 + 0.6T4 + 1.0T5$$

Where:

Zeta (ζ)	The Altman’s Z-Score.
T1	Working Capital / Total Assets.
T2	Retained Earnings / Total Assets.
T3	Earnings Before Interest and Taxes / Total Assets.
T4	Market Value of Equity / Total Liabilities.
T5	Total Sales / Total Assets.

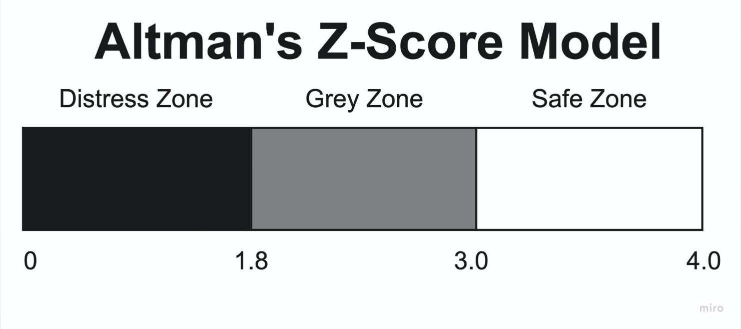
The usefulness of the original Z-core measure was limited by two of the ratios. Obviously, if a firm is not publicly traded, its equity has no market value hence the score is not useful. To deal with this, there is a revised Z-Score for private companies:

$$\zeta_1 = 0.717T1 + 0.847T2 + 3.107T3 + 0.42T4A + 0.998T5$$

The fifth ratio is *Asset Turnover* (T5). This ratio varies significantly per industry but, because of the original sample, the Z-Score expects a value that is common to manufacturing. To deal with this, there is a more general revised Z-Score for non-manufacturing businesses:

$$\zeta_2 = 6.56T1 + 3.26T2 + 6.72T3 + 1.05T4$$

Note that the revised version has slightly different zones of interpretation. This model can be applied in credit rating with the use of liquidations.



Altman's Z-Score Model zones.

In the initial test on a two year perspective the model showed an accuracy of 72% in predicting bankruptcy, and it returns a false positive of six percent. On a one year perspective it returned a false positive of $15\% \; to \; 20\%$. In subsequent test over 31 years up until 1999, the model was found to be $80\% \; to \; 90\%$ accurate in predicting bankruptcy one year prior to the event. Today it is used by Morgan Stanley to find underperforming stocks. A company with an Altman Z-score of less than 1 tends to underperform the wider market by more than four percent.

In the TradFi world, the score is usually computed with cash flows, assets, margins and earnings taken into account. DeFi requires a different approach with some similarities to the TradFi approach. By conducting on-chain analysis is it possible to subtract earnings and volume of dApps which in turn can be used to recreate a DeFi version of the Z-Score model.

Purpose of this paper

The aim of this paper is to provide a market overview of a relatively undiscovered service that could make the ecosystem advance considerably. We hope that this paper can serve developers and investors as an overview of what is working, what has failed to work, and what is in development in the field of credit rating for crypto. We have explored on-chain, off-chain, and other approaches to credit rating done by existing projects.

Every chapter is dedicated to an umbrella of credit rating solutions followed by projects that fall under that category. For example, the first chapter is *Third Party Risk Assessment* followed by a summary of the approaches deployed by Credora, Cred Protocol, and Teller Finance.
With this approach, we hope that it will be possible for the reader to properly focus on specific solutions considering the opportunities and obstacles they present.

These classifications are of course a simplification. Approaches can implement and even straddle different dynamics across these categories, but this framework provides a useful heuristic for analyzing the vast and varied approaches to the credit rating problem.

Third-party risk assessment

One of the more obvious solutions for DeFi is the implementation of KYC practices by a third party in order to facilitate trustworthy credit rating. This way, credit rating is done similarly to the TradFi world, where a neutral third party is trusted with the task to evaluate the creditworthiness of the borrower. Effectively, this means that the credit rating is outsourced and may exclude common standards. The classification is often done in a case-by-case approach using a diverse range of systems, policies and approaches that vary per protocol.

If this solution is adopted, based on our research we recommend:

- to design an explicit third-party and/or supplier risk assessment framework, including a definition of ownership, governance and articulation of risk appetite that will lead to alignment among internal stakeholders;
- to extend the scope to all third parties and apply risk-based segmentation to determine the level of control required;
- to apply a proactive and comprehensive approach to third-party risk assessment, including ongoing monitoring and escalation processes, even if it is outsourced;
- to invest in tools like data management systems, end-to-end workflow tools and analytics to increase the efficiency of and ensure consistency in the process.

We can define two subcategories of rating: third-party and protocol specific.
The former tends to be more accurate and the latter more decentralized. There are certain trade-offs between the two approaches. Take for example Credora, which has shown market fit and quite a few protocols, such as Maple and Atlendis, have adopted its solution for the rating of their borrowers. The protocol is an established authority in the institutional lending market, because of its privacy-based solution and successful network effect. The main problem here is scalability and permissionlessness. Credora requires parties to request access and thus isn’t suitable (yet) for broader adoption by retail. Additionally, the protocol is quite centralized in that regard, making it less appealing for fanatic proponents of antifragility and decentralization.

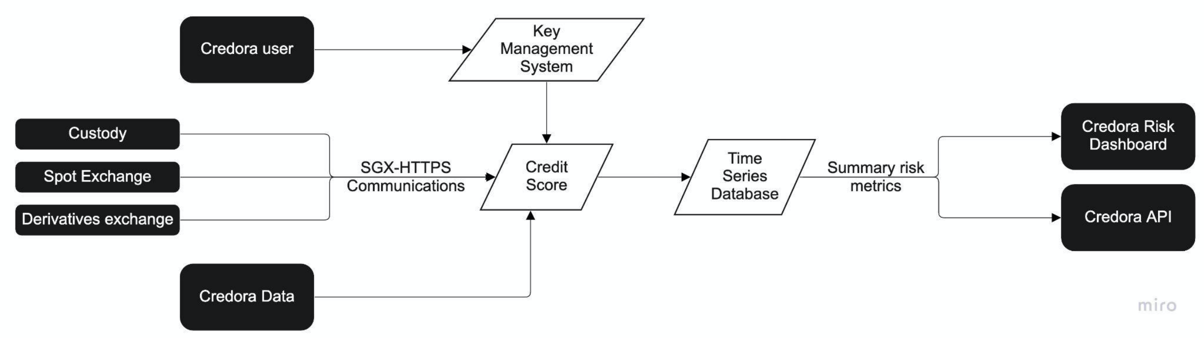
On the other hand, a protocol-specific solution like Cred Protocol performs analysis through the use of machine learning. This panacea allows them to compute large datasets thus making the protocol scalability-oriented but can be inaccurate by the lack of inclusion of certain data that is not read by the AI. Other implementations of this solution are ARCx and Teller finance.

Credora (Formerly X-Margin)

credora	
Website URL:	https://credora.io/
Development state:	*Access upon request.*
Integrated on:	*Clearpool, Maple, Friktion, LedgerPrime, Zest, Auros, Cega, Folkvang, Atlendis, Wintermute, Maven11, dAMM, Ribbon…*

Credora offers a privacy-preserving credit evaluation solution for institutions. They have built their infrastructure on top of Zero-Knowledge Proofs that allow their clients to give insight into their portfolio and balance sheets without having to give up exact details. This promotes privacy and protects sensitive information from malicious insiders. Credora is able to offer secure credit risk scoring by shielding computations in Intel SGX enclaves and performing Homomorphic Encryption-based Zero-Knowledge Proofs to offer cryptographic proof of security, computation and encrypted input.

This is done by leveraging a combination of secure Intel SGX enclaves and cryptographic proofs that prove a) the data came into the enclave encrypted, b) the data was only computed in a specific way, and c) no data was leaked by the enclave. This solution still presents dependency on hardware-based Trusted Execution Environments (*TEEs*) creating certain risks that are hard to mitigate. Assuming that hardware manufacturers are honest and produce reliable hardware, they are of course incentivized to do so by reputation and business-wise approaches, but the risk remains. Credora has been trying to alleviate this risk by exploring a new frontier for privacy-preserving computing such as the use of the cryptographic scheme Functional Encryption (*FE*).



Credora Architecture, "Privacy-preserving Credit Scoring via Functional Encryption"

Credora calculates a variety of risk metrics on each user's portfolio, including equity, balance, margin usage, and maximum loss (SPAN or VaR calculations). The final score institutions receive is a number from $0\ to\ 1000$ and is based on three categories:

- [200] **Operations and Due Diligence** - measuring corporate and operational risk;
- [200] **Financial Analysis** - evaluating a borrower's reported financial data;
- [400] **Risk Monitoring** - evaluating in real time a borrowers' asset and liability visibility.

Grade	Score Range
AA	$850 - 1000$
A	$700 - 750$
BB	$550 - 700$
B	$400 - 550$
C	$200 - 400$
D	$0 - 200$

Credora's rating categories

Based on the credit score institutions receive, they are then rated from *D* to *AA*. The real-time credit valuation and credit score by Credora allow them to calculate a maximum *borrowing capacity*. This metric provides clear guidance for other protocols and institutions. The borrowing capacity targets the maximum amount of borrowing that is feasible.

The current roadmap of the company is to enhance functional encryption in production to give further guarantees of neutrality and privacy to their clients. The company is heavily backed by VCs, with the last round being a Series A worth $\$8\ million$.

Pros	Cons
Sensitive information is kept *secret* as their product is built on top of Zero-Knowledge Proofs. This also tackles the problem of malicious insiders.	Charges a fee upon using which results in the addition of another cost besides the cost of capital for the borrower.
They offer a trusted service that can be used as infrastructure by other protocols that can then focus on building.	The rating criteria is tailor-made for institutions and it could not be as complete for individual borrowers.

The three layers of rating offer a complete overview of the borrower.	The protocol ends up being quite centralized and could benefit from the creation of its own chain.
Investing in Research and collaborating with academic researchers to innovate their product.	
Exploring ways to reduce their weak points by using Functional Encryption.	

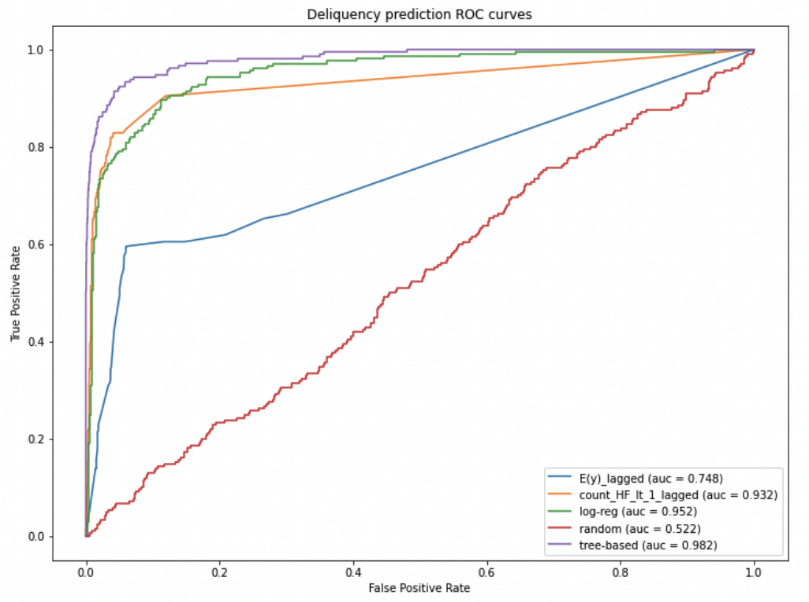
Cred Protocol

Website URL:	https://www.credprotocol.com/
Development state:	*Beta whitelist.*

Cred Protocol scores risk by correlating on-chain account history with the propensity to liquidate loans. It does so by using *machine learning* to assess time-based account attributes and analyze a user's past transaction behavior. They generate a *health factor score* that predicts the likelihood of future liquidation for a single address which usually is one of the strongest baseline creditworthiness predictors. The health factor is calculated with the following formula:

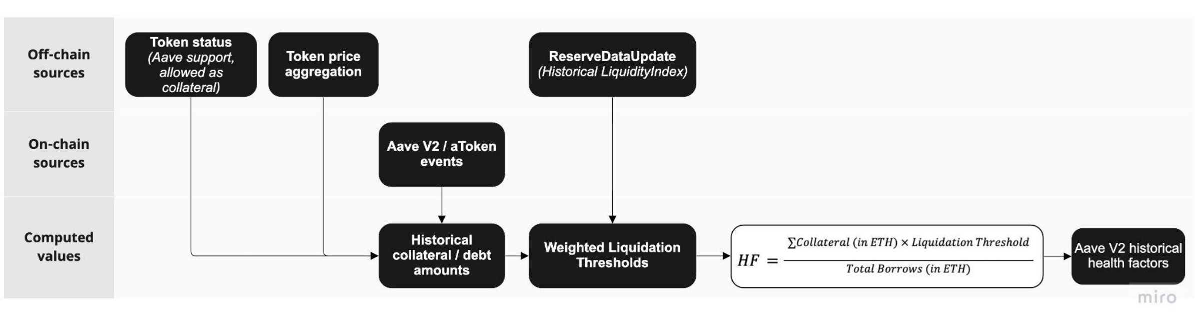
$$HF = \frac{\sum \quad Collateral\ (in\ ETH)\ \times\ Liquidation\ Threshold}{Total\ Borrows\ (in\ ETH)}$$

As for this moment, the score is based on a ML model that takes the behavior of Aave V2 users over time and predicts their propensity to get liquidated. This is possible thanks to the Aave V2 Health Factor Dataset, which contains every account's position on the platform and health factor information at 15 minute time intervals. This model takes into account an account's age, aggregations of the time series of its historical health factors and interactions with the Aave protocol, besides keeping track of the assets it borrows and keeps as collateral. They remove all of the positions that took span over a period minor of ten days, as they are marked as "short-term" positions, and usually resemble flash loans effectuated by smart contracts as opposed to accounts themselves.



The evaluation in their model measures the area under the receiver operating curve (AUC) which statistically quantifies the model's ability to score positive examples predicting if an account can a) randomly deviate from uniform or b) have historical delinquency frequency. The model was trained with over 34,000 rows of data and five different approaches were considered: *random*, *E(y)_lagged*, *count_HF_lt_1_lagged*, *log-reg*, and "*treebased*. The results can be found in the image above. As you can see the purple line depicting *treebased* classification shows the highest likely hood of predicting position delinquincy.

They are now collaborating with *Aave* V2 and are backed by *Alliance Ventures, GSR, Volt Capital, AngelDAO, Robot Ventures, imToken, and Luno Expeditions*. As of their roadmap, they plan to expand to other protocols such as *Compound* and *MakerDAO*.


Off-chain sources
On-chain sources
Computed values
Token status (Aave support, allowed as collateral)
Token price aggregation
ReserveDataUpdate (Historical LiquidityIndex)
Aave V2 / aToken events
Historical collateral / debt amounts
Weighted Liquidation Thresholds
$HF = \frac{\sum Collateral\ (in\ ETH) \times Liquidation\ Threshold}{Total\ Borrows\ (in\ ETH)}$
Aave V2 historical health factors
miro

Cred's pipeline to create Aave V2 health factor dataset

Cred's core mission is to quantify risk in order to provide credit scoring at scale. They have a proprietary on-chain oracle on Arbitrum that projects can integrate to incorporate Cred's credit rating to their mechanics.

Pros	Cons
Uses machine learning to evaluate on-chain activity history making it possible to analyze large sizes of data.	Very incomplete documentation and product still in beta - cannot be fully analyzed.
Collaborating with Aave allows them to have a huge dataset of loans.	Strongly relies on VC funding.
Partnered with Cornell university to foster research.	
Team with tons of experience in Web2 giants and previous exits in the startup world.	

ARCx

ARCx	
Website URL:	https://arcx.money/
Development state:	*Whitelist only.*
Chain:	*Polygon.*

ARCx Credit is a decentralized credit market on Polygon that offers dynamic loan-to-value (*LTV*) loans on ETH collateral that changes based on the users' credit score. To score their lenders, ARCx uses a DeFi Credit Score that assigns a value between 0 and 999 describing the credit risk of an individual wallet address based on their on-chain borrowing activity. This score is composed of three different components:

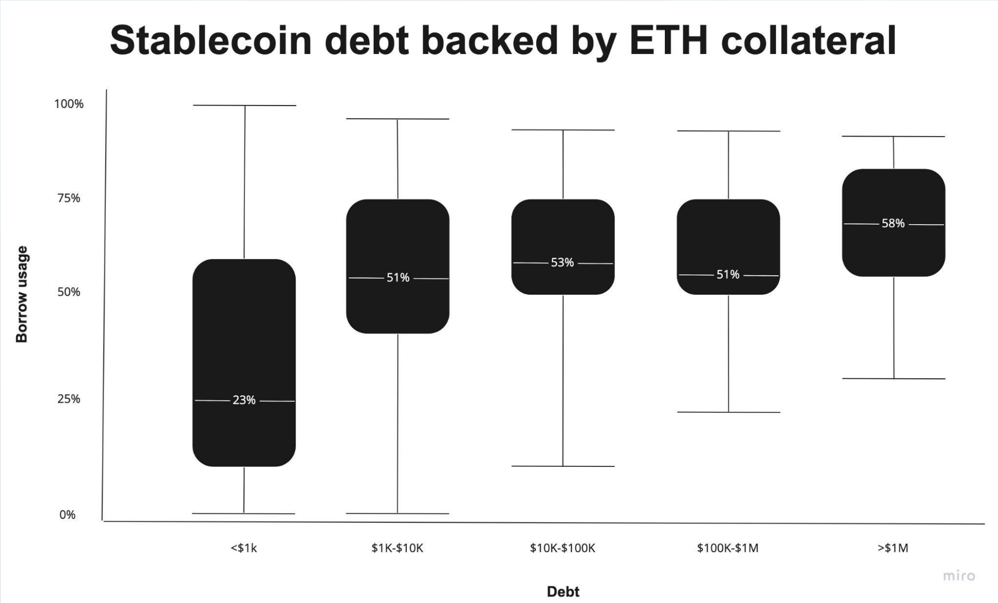
a) a **daily score reward**, that computes a LTV on the platform's vaults over the prior 120 days rating borrowers on their responsibility archetype assigning rewards points according to a rewards curve on a daily basis. This score component can give up to 999 points in total;

b) a **survival score reward**, that evaluates a borrower's ability to avoid liquidations on any third-party platform, subtracting points proportional to the liquidation density on a given day. This score component can give 300 points in total;

c) a **liquidation penalty**, that subtracts a fixed number of points for every day on which a liquidation occurs and only applies for 120, after which the penalty is removed. This score component can subtract 250 points per liquidation event on ARCx platform.

These score components are added together and capped at 999 points, which is the maximum score users can achieve. This gives any DeFi user a fair chance of reaching a maximum classification to benefit from the perks offered to higher scoring users. For example, the higher a DeFi credit score, the chaper the loans can be. Users can lose points if the daily score reward grows slower than the rate at which the points are expiring, i.e. 120 days. This can happen if users stop borrowing entirely or in excess from their critical point, i.e. borrow usage is greater than 90%.

The platform suggests borrowers an optimal borrow usage of 60%, based on which an user's DeFi will grow accordingly. Since the collateral is only accepted in ETH, this requires users to balance efficiency with risk exposure given by the asset's volatility. The suggested optimal borrow usage of 60% originates from a yet to be published analysis on the safety buffer of users' collateral in Compound. Results from this research show that 60% was approximately the mean, especially for larger debt positions. Another consideration was that it intuitively provides a reasonable compromise between borrowing safely and under-utilizing collateral. The figure is optimal as it makes the most out of the collateral while also protecting against significant price drops of the underlying collateral.



Borrowers on Compound, ARCx Analysis

The mechanics of the protocol require users to post collateral into a vault (*WETH-A*). If users have grown their DeFi credit score through responsible borrowing then they will unlock greater capital efficiency up to 90% of LTV is the score is positive, 95% of TVL if the score is greater than 500 and 100% if the score is greater than 750 points.

Vault	Score threshold	Capital efficiency
WETH-A	0 +	Up to 90% LTV
WETH-B	500 +	Up to 95% LTV
WETH-C	750 +	Up to 100% LTV

ARCx borrower vaults offering

The three vaults design choice does not have a use rather than facilitating user experience in meeting the requirements of progressively and frictionlessly unlocking greater capital efficiency.

The fee structure includes a 0.2% borrow fee, a 2.5% interest rate, and a 10% liquidation fee. Interestingly, they allow users to get self-managed liquidations in which case 100% of the revenue is kept by ARCx. Currently, 90% of the interest and borrow fees are returned to lenders while 10% goes to ARCx and is then used to fund further development and growth, meaning LPs get a 0.18% borrow fee and 2.375% interest on their pooled assets plus any applicable liquidity mining incentive. This does not apply in the case of liquidations, on which ARCx retains a 50% quota, instead.

Note that as borrowers improve their DeFi credit scores and borrow at increasingly higher LTV ratios, the platform exposes itself to a greater chance of losses from unprofitable liquidations. This does not benefit LPs at all as if the compensation does not come from the borrower’s excess collateral, the offset is taken from the pool representing toxic debt.

The DeFi Credit Scores are combined into Merkle Trees and published on every blockchain supported by the protocol on 24 hours windows. This allows credit scores to be chain agnostic, as the same score is recorded on each blockchain.

The protocol also issued a ARCx governance token which is currently used to vote on expenditure from the treasury and has an hard cap of 100 *million*. ARCx is backed by *Dragonfly Capital, Scalar Capital and LedgerPrime*.

Pros	Cons
Fees and interest rates are competitive with both	After 120 days liquidation history is canceled,

profits and losses shared by LPs.	meaning that a malicious user can just wait to have a better score.
Able to offer greater capital efficiency to borrowers.	A user’s positive borrowing history does not implicate positive future behavior and there might not be incentives to repay back loans if liquidation does not become a dominant strategy.

Teller Finance

Teller	
Website URL:	*https://teller.org/*
Chain(s):	*Polygon.*

Teller allows borrowers to bridge off-chain onto on-chain loan requests allowing lending on reputation. The platform is similar to a peer-2-peer (*P2P*) loan order book and consists of three user categories:

a) owners - parties who build on top of the platform creating their own marketplace and choosing their own governing parameters (payment cycles, default periods);
b) lenders - users who provide capital to the platform (may require to go through KYC);
c) borrowers - users who want to take out unsecured loans (required to go through KYC).

The verification of borrowers and lenders is done via Ethereum Attestation Services (*EAS*) plus additional KYC through *Hypernet* and users may be required to connect their bank account to the platform to access a loan. This system allows Teller to stay regulatory compliant.

Teller's loan service is called *SG Loans* and is aimed toward personal unsecured loans. Borrowers can borrow based on their credit rating from the *Singapore Credit Bureau*. The platform works as an order book, enabling borrowers to associate their off-chain credit rating data with on-chain loan requests and matching lenders and borrowers with similar bids/asks. Currently, the markets on Teller should be consumer credits for consumers that want fast capital for small purchases, residential mortgages, and small business revenue-based financing for business-2-business loans. That being said the loan books are relatively unpopulated and we could only find three ongoing borrowers.

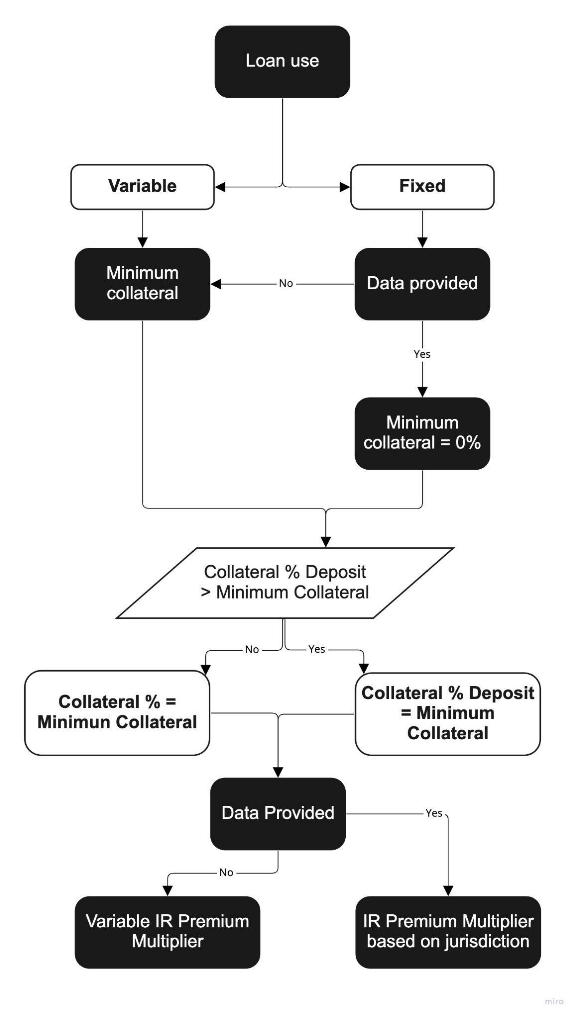
The protocol is autonomous thanks to its algorithmic nature and their tech such as Teller's credit risk algorithms (*CRAs*), which serve as the foundation for managing the protocol's liquidity pools, also known as autonomous Teller markets (*ATMs*).

The risk parameters are handled by the protocol and follow an Arrowhead's logic flow where:

$$Interest\ rate\ per\ asset\ \ = rfToken\ IR + Risk\ Premium\ IR$$

rfToken IR are asset specific risk-free interest rate accounting for said assets and risk premium IR is the global asset-specific additional interest rate to account for risk associated with fully unsecured loans.

In future iterations of the protocol, Teller validators will utilize both secure enclaves and zk-Snark technology to enhance data privacy and protection further.


Loan use
Variable
Fixed
Minimum collateral
No
Data provided
Yes
Minimum collateral = 0%
Collateral % Deposit > Minimum Collateral
No
Yes
Collateral % = Minimun Collateral
Collateral % Deposit = Minimum Collateral
Data Provided
Yes
No
Variable IR Premium Multiplier
IR Premium Multiplier based on jurisdiction
miro

Teller Finance Loan Framework

Pros	Cons
Able to safely offer unsecured loans for borrowers.	Relies on traditional forms of credit rating - does not bring any innovation.
Regulatory compliant thanks to the heavy KYC practices required.	Requires both parties to go through KYC - unaligned with crypto values. In order to get a loan, users need to connect a bank account but data remains private.
	Resulted in not getting too much traction as it

	currently only features three borrowers.
	Relying on the Amazon Web Service (AWS) and the Google Cloud Platform (GCP).

Non-Fungible Credit Scores (*NFCS*)

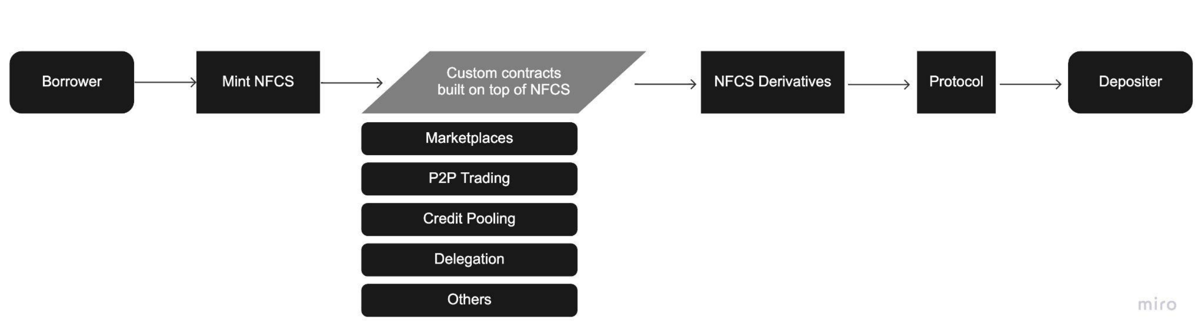
A common way of understanding one's creditworthiness is as a register of all past transactional behavior and financial decisions. The rating is implicitly done based on whether the borrower followed regulatory rules and conducted safe practices of risk management. Traditionally, this type of information is only in the hands of certain parties, most often banks, who are responsible for the settlement of financial transactions. This is contrary to the blockchain which is fully transparent, publicly visible and allows anyone who wishes to perform some kind of credit rating on blockchain wallets.

This leads to another interesting approach to crypto credit rating, one that is done entirely on-chain. There are a couple of projects on the market that bundle on-chain data into an NFT and have a score tied to that information. This score could allow the user to take out a loan or give access to certain privileges on a platform, e.g. more favorable interest rates.

This technology, also referred to as non-fungible-credit or non-fungible-token credit profile, is often an ERC-721 token since the standard allows for:

- the decoupling of data collection and data ownership from the credit scoring and credit issuing processes;
- the decentralization of scoring, where various credit-scoring backends can score bundled addresses independently;
- the ability for a borrower to apply for credit or access other use cases that operate with an on-chain reputation on other DeFi platforms besides from the issuer;
- use cases that require proof of multiple address ownership;

NFCS operates similarly to TradFi's credit bureaus like *FICO* where the score belongs to the user, but the user does not control it. This tech allows for a different user experience on borrowing platforms and in the DeFi ecosystem, introducing a whole world prior to a loan request:



NFCs use cases

Challenges for this type of tech are that protocols need to be sure that the NFTs are dynamic and soul-bound at the same time, ensuring that the credit scores are non-transferable while they must have the ability to be updated. There is also the risk of not capturing all the associated wallets which may have adverse activities/transactions that will negatively impact a user's credit score. Cherry picking is a risk that can materialize and is another blow for implementing this solution.

To be implemented in a responsible and effective manner, NFCs:

a) must implement a feature by which addresses/accounts that are already part of an NFCS bundle cannot be used in another NFCS bundle;
b) must require users to confirm ownership of each address added to the bundle via nonce signature;
c) must be limited to one per wallet;
d) must not be transferable (see SBTs below);
e) must allow users to add new addresses but not to remove them.

The most interesting protocols offering this solution are Spectral, RociFi, CreDA, AlphaWallet, and Quadrata.

Soulbound tokens

Vitalik Buterin recently introduced in a whitepaper entitled "Decentralized Society: Finding Web3's Soul" the need for the introduction of soulbound tokens (*SBTs*).
SBTs are non-transferrable identity and reputation tokens that allow individuals to verify all of their information such as their education, work history, credit score, medical history, professional certifications, etc. — using blockchain technologies.

SBTs seem to be a more streamlined and trustworthy way of verifying information but they can be a dangerous tool if in the wrong hands.

If we compare SBTs to NFTs, recall that every NFT has its own identification code and metadata, meaning that every NFT is unique and the data it contains cannot be falsified. Regular NFTs can be sold or sent to any address, making them untied to any particular entity/person.

On the other hand, Soulbound tokens are just permanent, non-transferable NFTs, meaning that they can't be given away or taken from your private blockchain wallet.

SBTs	NFCs
Are non-transferrable.	Are transferable. (On a general basis, depends on the issuer)
Suited for identity verifications.	Are used for proving ownership of specific requirements.
They may allow for the creation of a model that enables the restoration if lost.	Almost impossible to recover if private keys are lost.

Some SBTs may be used like real-life achievement badges, as their beginnings come from video games achievements. However, we see this technology to be much more useful to be used for personal certifications, like degrees and awards, but also for credit rating.

In particular, while standard Non-Fungible-Credits are transferable, bundling all of the wallets' data in an SBT could resolve the secondary market problem for NFCs.

Interesting projects that are currently building on top of the soulbound concept include:

a) **Sismo** - building ZK Badges that are Non Transferable Tokens (ERC1155), aka Soulbound tokens. These ZK Badges will be be used for reputation aggregation and privacy access;
b) **Rabbithole** - building a guide users through a set of on-chain tutorials after which they will be eligible to create a "RabbitHole Certificate", which represents users' skill set;
c) **Binance** - building their own SBT called Binance Account Bound (*BAB*) that is non-transferable, has no monetary value, and is the first-ever SBT issued on the BNB Chain;
d) **Optimism** - using SBTs to attestate voting rights for their bicameral governance model;
e) **GoldFinch** - issuing SBTs to users who passed the 'Unique Entity Check';
f) **Radix** - which anticipated Vitalik using SBTs to set the state transitions in/out of vaults to be restricted. Through this mechanism they are able to edit the time users can use a token;
g) **Masa** - building a decentralized credit report as a soulbound NFT;
h) **Noox** - building a platform where users can mint their Web3 achievements/ actions as Soulbound NFTs;
i) **Proof of Humanity** - launching a social identity verification system for humans on Ethereum;
j) **3xcalibur** - using SBTs as proof of participation in the discounted seed sale.

Most common use-cases for SBTs could be identity management, governance rights, on-chain credit scores, and proof of attendance badges.

Spectral

Spectral	
Website URL:	https://www.spectral.finance/
Development status:	*Yet to be launched.*
Token:	*$SPEC.*

Spectral offers credit scoring using artificial intelligence through a multi-asset credit-risk oracle (*MACRO* score) and Non-Fungible Credits (*NFCs*).

The *MACRO score* is an on-chain credit score that represents one's credit standing and mainly takes into consideration on-chain data. The data of the score is grouped into five categories, these being payment history, liquidation history, amounts owed and repaid, credit mix and length of credit history.

The score ranges from 300, which stands for a bad credit standing to 850, which means that a user has a good credit standing. MACRO scores evolve quite frequently as on-chain information changes over time. The on-chain data analyzed by the protocol consists off:

a) the transaction history – the protocol takes the history of the transactions on the Ethereum network and screens the wallets an user has transacted with and the volume of ETH transacted;
b) the liquidation history – as of common use, liquidations are conceptually interpreted as a proxy for defaulting on a loan and used to collect information about risk management types;
c) the amounts owed and repaid;
d) a credit mix – the protocol considers the variety of dApps a wallet has interacted with;
e) the length of credit history – a longer credit history increases one's MACRO score. This can be seen as an incentive for people to batch old addresses into the platform as they can higher the score and Spectral can get to learn more about one's history.

The analysis of the on-chain transaction history is also represented with a health factor, which is proportional to the ratio of the value of all collateral supplied to the value of all outstanding borrowed funds:

$$Health\ factor = \frac{Value\ of\ the\ collateral\ supplied}{Value\ of\ all\ outstanding\ borrowed\ funds}$$

In their scoring system an account typically becomes subject to liquidation once the health factor goes below one and they take into consideration the past health factors when calculating a new *MACRO* score. One's health factor was introduced by Compound. Spectral does not only take into account one's current health factor in the DeFi ecosystem but also the entire history of past health factors

Standing out in their on-chain analysis they also analyze one's historical interactions with rug pulled tokens- by the idea that one's interaction with riskier smart contracts can be indicative of a higher risk profile. Rug pulls are defined as the act of malicious individuals creating a token with the intent to scam. The nature of these tokens permit to associate the high-risk high-reward nature of DeFi's tokens with one's risk appetite, i.e. the more an user has interacted with rug pull smart contracts, the more their MACRO score would be affected.

A user's on-chain transaction history is then bundled in a non-fungible credit (*NFC*), which is an ERC-721 token that allows users to bundle wallets and sync their on-chain transactional history. Spectral allows users to bundle various addresses before creating the NFC. Doing so, the users' MACRO score is integrated with all their addresses. A transaction is signed to prove ownership of the funds and addresses included in the NFC.

Once a credit has been tokenized, the NFC is programmable and composable. This allows for custom credit marketplaces to be created and other financial products, like Web3 login, securitized debt, credit staking and delegation.

The protocol also takes advantage of the open-source nature of Ethereum to collect and extract a broad dataset that comprises all the on-chain borrowing transactions and behavior on leading DeFi protocols. This numerical data is then bucketed into discrete categories and used to expand the protocol features. Also, since there is no default event, the protocol uses liquidations as a proxy, an event which is comparable to a write-off in TradFi. Therefore Spectral converts the traditional PD/EAD/LGD expected loss framework into PL/EAL/LGL in which the loss given liquidation (LGL) is almost always zero due to the high collateralization levels. This approach assigns liquidations sufficient value to be used for risk modeling, since they imply that the borrower was too aggressive, couldn't handle market fluctuations or did not take the necessary actions to prevent the event from happening. This, of course, must come with the notion that liquidations are not considered in isolation for the MACRO score.

The machine learning algorithm Spectral uses to generate scores performs several iterations to select the best subset of features following the approaches of:

a) **correlation evaluation** – that selects features that exhibit high correlations among themselves to then exclude them, ensuring that none of the features represent the same information that could impact the interpretability of the final model;
b) **variance analysis** – which excludes features with a very low variance among observations as they do not add value to the predictive power of the algorithm;
c) **feature importance derivation** – that uses several well-established metrics to identify and rank the features. The model validation is then conducted with several techniques such as

traditional validation metrics (recall, F1 score, AUROC, Gini Index…), backtesting and stress testing and distribution checks.

The MACRO score is then generated from the model and evolves continuously.

On Spectral, computation is done off-chain and only proofs are produced on-chain. There's no reason why these proofs of computation should not extend to arbitrarily complex computations cast in a form of a zk-proof-setup. The structure Spectral uses is a decision tree and is very similar to a Merkle Tree. Spectral first trains the decision tree using public blockchain activity, then merkle-izes the decision tree to allow one to cryptographically commit to the decision tree and finally produces proof that the credit score was calculated honestly. Zk-Snarks are used to hide the particular paths of the decision tree and to prevent users from collaborating to learn model parameters.

Spectral's roadmap shows their interest in implementing credit staking, by which staking an NFC and not defaulting grants a user can get yield or better rates; securitised debt packages; and credit delegations based on the Euler Beats model.

The team is composed by 27 people and the protocol has gone through several funding rounds concluding with a series B for a gran total of $23 *mln*. They have launched their Beta in October and got decent traction from the start. Pre-seed investors include *Rarestone Capital, Galaxy Digital, Maven 11, New Form and the DeFi Alliance*.

Pros	Cons
They allow users to bundle different addresses to get a more complete credit score.	Bundling addresses on Mainnet can be expensive.
They analyze a wallet's historical health factor and rug-pull relationships.	A bundle cannot have new addresses added or old addresses removed once it is minted.
They collaborate with TradFi specialists on loans (Raymond Anderson).	NFCs concept is very similar to other protocols.
Their solution facilitates a composable credit score primitive.	An user can decide not to include a particular address in a bundle. (Cherry-picking problem)
Their credit risk oracle could serve as a middleware solution for programmable creditworthiness across ecosystem.	Strongly dependant on VC funding.
Having proprietary lending pools.	At launch the MACRO score will only allow a maxiumum LTV of 120%, meaning that they will only allow overcollateralization.
A users MACRO score gives access to variable rates.	

Team with web2 giants experience and ivy league degrees.

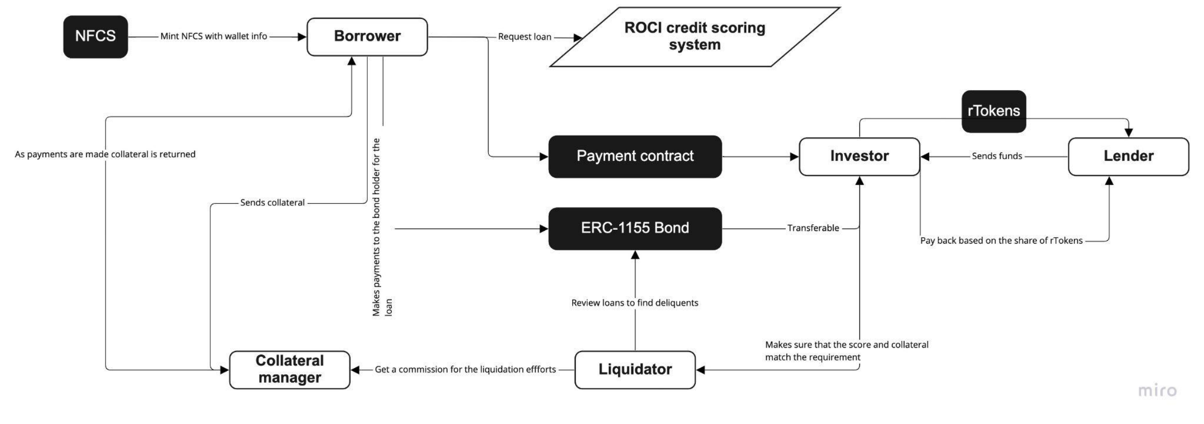
RociFi

RociFi	
Website URL:	https://roci.fi/
Development status:	*Testnet - scheduled launch for Q3 2022.*

RociFi is an undercollateralized credit protocol on Polygon. They offer three main products: non-fungible-credit-scores (*NFCS*), ScoreDB and CreditScore. While the last is an off-chain service, NFCS is an NFT token containing the list of all of Ethereum addresses ever signed by a user, and ScoreDB is an oracle that connects off-chain credit score services through ChainLink, handling the fetching off-chain data services and executing score-sensitive logic.

In order to borrow from RociFi, users need to be credit risk rated by the protocol's credit risk scoring (*CRS*) system. In order to receive a CRS, users must mint their NFCS token first, which are ERC-721 tokens minted on mainnet, created by calling the NFCS.mintToken function and then used to generate a personal credit risk score. The credit risk score is a number between $1 \; and \; 10$ and it is generated off-chain by the ROCI credit score API.

Non-fungible-credit-scores contain a set of user's data such as the addresses, borrowing history on RociFi, CRS updates, and they are immutable once generated. The RociFi NFCS is considered to be a credit passport that catalogs user's on-chain behavior on an interpretable scale from $1 \; to \; 10$; with the lowest being the most creditworthy and ten being the least. RociFi currently only offers users to borrow USDT, USDC and DAI; while ETH and WBTC can only be used as collateral.


NFCS
Mint NFCS with wallet info
Borrower
Request loan
ROCI credit scoring system
rTokens
As payments are made collateral is returned
Makes payments to the bond holder for the loan
Payment contract
Investor
Sends funds
Lender
Sends collateral
ERC-1155 Bond
Transferable
Pay back based on the share of rTokens
Review loans to find deliquents
Makes sure that the score and collateral match the requirement
Collateral manager
Get a commission for the liquidation efffords
Liquidator
miro

RociFi's flow

Investors play a key role in their business model as they are vital to ensure proper liquidity to the protocol in the credit pools and they release the loaned asset from the liquidity pool to borrowers and route repayments from borrowers to lenders. The protocol bases itself on four types of tokens, this being a) debt tokens, which are standard ERC-20 tokens representing a lender's share in a particular lending pool; b) bond, which are ERC-1155 non-fungible tokens corresponding to a specific loan and are parameterized by principal amount, collateral type and amount and the loan maturity date; c) asset tokens, which are ERC-20 tokens used for borrowing; d) collateral assets, which are ERC-20 tokens to be put as collateral.

RociFi also integrates a credit risk oracle, which takes part in both the generation of a loan's LTV and a user's credit score connecting to the off-chain credit scoring analytics and price feeds. The off-chain credit scoring analytics works by fetching on-chain data collected about users into a machine learning model that returns a probability that a particular user would have their loan result in default if given access to a loan.

Interestingly, RociFi also considers another source of credit risk; Fraud. Which can be conducted in multiple possible shadows including exploits, attacks, scams, and phishing. Addresses associated with these types of fraud activities in the past are considered by the protocol to be more likely to simply run away with funds if given access to credit. Their off-chain fraud analytics are based on modern approaches that combine graph theory and machine learning.

The borrower interest rate on RocFi is calculated as the sum of the risk-free rate (R_f), the risk premium(R_p), and the volatility charge (V_c):

$$Borrower\ interest\ rate = R_f + R_p + V_c$$

This interest rate is a derivative of the Capital Asset Pricing Model (CAPM), and to do so RociFi utilizes a linear model of the following form, with the rate for lenders acting as spread on top of the base rate for which would make the loan attractive to a lender based on opportunity costs and perceived default risk. The formula is very similar to Aave's.

$$R_l = R_f + V_c + \frac{U - U*}{U*} R_s$$

In their roadmap pipeline, they declare to be in conversation with a DID project to integrate their product as a datapoint for other protocols to perform individual assessments on users, to be working on the deployment of other ERC-20 Tokens and NFTs as collateral, and to eventually move to be a DAO as they grow.

They have conducted fundraising rounds for a total of \$2.7 *million* from *ArringtonXRP Capital, Signum Capital, Nexo, GoldenTree, LDCapital,* and *SkyNet Trading*.

Pros	Cons

They fetch data from different EVM chains.	The NFCS concept is very similar to Spectral’s.
They craft a borrower credit risk scoring system (CRS) that ends up minting an NFCS.	Obscurity about the effectiveness of ‘social recourse’ in an industry where most are pseudo-anonymous.
Audited by Chainsulting and Certik (not available).	Unclarity about the importance of t addresses outed as non-repayers for other protocols.
Interest rate rewards lenders for risking capital on undercollateralized loans on the top of the risk-free rate.	Strongly relies on VC funding.
Takes into consideration Fraud risk by considering past address relationships.	Borrow limit for undercollatearlized loans (500 USDC) is very low.
Borrowers that will be eligible for the collateralization must consent to ‘social recourse’, i.e. they will be publicly exposed as non-repayers in case of loan default.	

CreDa - Credit Data Alliance

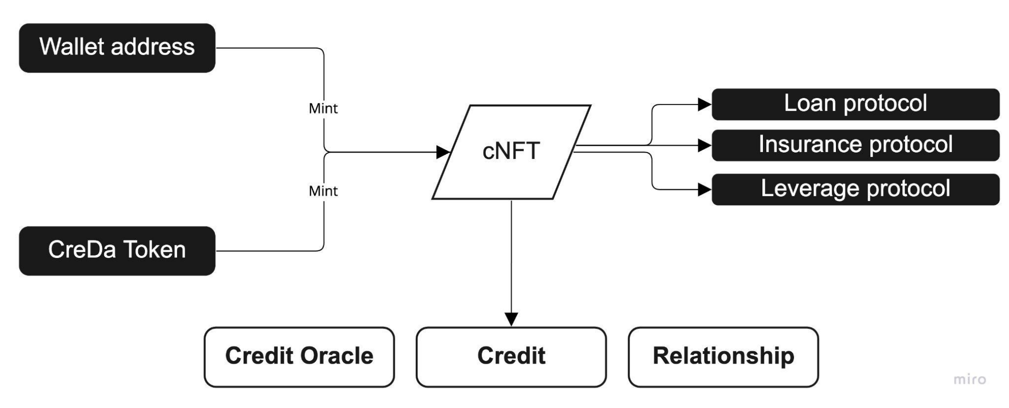
CreDA	
Website URL:	https://www2.creda.app
Chain(s):	*Arbitrum, BNB chain, Elastos SC.*
Token:	*$CREDA.*

Credit Data Alliance (*CreDA)* offers both credit scoring and yield-farming on three DeFi blue-chip pools. Using on-chain data, CreDA Credit Oracle, the protocol's proprietary oracle, computes credit scores utilizing transactions across multiple chains, which are Ethereum, Arbitrum, Binance Chain, Fantom, Polygon, HECO and OEC.

They provide on-chain credit ratings by minting a user's credit profile into a non-fungible token (*cNFT, credit NFTs*). This token enables the user to unlock preferential rates and incentives across a variety of use cases, for instance, reduced borrowing rates. To conduct their credit rating, they use artificial intelligence to fetch blockchain data and assess users' activity in a few EVM chains, being based on the decentralized identifier protocol (*DID*) and their proprietary CreDA *Credit Oracle*.

The on-chain analysis they conduct breaks down:

- the historical user assets, fetching data from the asset holdings across all blockchains, the length of time owning these assets, and the size of the assets; bonding them under a unique *DID*;
- the historical activity of bound wallets, following the transactions under a DID, the participation across DeFi projects, the funds involved in on-chain transactions, the trading networks and other on-chain metaverses social network activity under that DID. This data represents whether someone is an active on-chain user and their trading preferences;
- the on-chain behavior of an address, screening the participation in DeFi programs;
- the loan participation, getting data on the amount of time participated in loan programs, whether liquidated or not, the value of the collateral.



CreDa's flow

Both the decentralized credit rating and the lending algorithms run on the data contained in the cNFT. Each on-chain credit NFT is generated with a DID at its core and includes a) the status of assets across all wallets bundled with the DID; b) the transaction history and present status on each DeFi protocol; c) the credit rating calculated by the credit oracle; and d) the CREDA tokens minted by an user onto their cNFT. This model turns out to be quite scalable, upgradable, and usable for a potential "metaverse credit network".

CreDA introduces a new contract form in DeFi that they have called "credit contract". This contracts allows for two use-cases: a) zero collateral loans; and b) credit insurance. It is unclear how they plan to allow these two use-cases and how this type of contract is different from traditional smart contracts.

The CreDA credit oracle will then generate relative credit ratings for users that range from zero to one thousand. $CREDA is the platform's native token that is airdropped to users in a locked status after they have been successfully credit scored. The unlocked version of the token serves the following purposes: a) oracle service, as third party protocols need to use CREDA as a basic fee token to utilize the service; b) mint cNFT, as users can both mint and upgrade the non-fungible tokens with CREDA; c) membership, as holders obtain protocol revenue and discounts on interest rates and transactions; d) community governance, d) liquid pool staking.

Pros	Cons
Allowing the minting of cNFT that aggregates a user credit profile and can be used to unlock preferential rates.	TradFi company structure with the CEO being a former Morgan Stanley executive.
On-chain activity analysis on different EVM chains.	Unclarity about the use cases of the cNFT.
Basing their credit rating on DID and a proprietary oracle.	Unclarity about the "credit contracts" allowing for zero-collateral loans.
	Their only selling point is NFCs, which result to

	be very similar to other competitors.
Partnered with CyberConnect to include social data in CS.	

AlphaWallet

AlphaWallet	
Website URL:	https://alphawallet.com/
Note:	*Not offering credit rating but token attestations that can be used in the field.*

Alphawallet is an open source self-custodial wallet. The Wallet offers ERC-721 token attestations that let users associate an email or mobile number to identify ownership of an asset on the blockchain, without revealing their identifier or address. This gives users additional reach and utility for their assets, allowing them to optionally use the blockchain, enabling a second market to exist under the control of the original ticket-issuing business.

Token attestations are Ethereum tokens that can be used without a pre-defined ETH address which opens up to use cases for non-Ethereum users to onboard in other fields such as vouchers, marketplaces, and online shops. These tokens use the TokenScript framework and hence become “smart” tokens.

TokenScript is a JavaScript/XML framework for blockchain tokens that allows token issuers and trusted authorities to enrich a token with a wide set of information, rules and functionalities. This permits users with little coding experience to use the package needed to access the token contract that runs on wallets as a mini dApp. The implementation of such a script allows an environment in which tokens can be used more securely and privately. TokenScript files are signed by the creator of the token smart contract or a trusted source with a public key. Wallets and dApps can import and verify the files and make sure users only get authorized TokenScripts from trusted sources.
In relation to credit rating, TokenScript can be used to know the token specific history with all details, to implement token specific rules, to trigger attestation processes and attestation transactions, and to display validated information about a token.

AlphaWallet has already partnered with DevCon on the development of an attestation-based Ticketing System and it is backed by Fenbushi Capital, UnityVC, Hashkey Capital, and Longhash Ventures. Team is fully known with both Web2 and Web3 experiences.

Pros	Cons
Token attestations allow them to market to non-Ethereum users expanding the TAM.	Company structure very similar to a Web2 one.
Team known and very experienced in Blockchain.	Strongly dependent on VC funding.
	Very incomplete documentation, and credentials required for accessing the investor slide deck.
	Undefined product market fit.

Quadrata

Website URL:	https://quadrata.com/
Chain(s):	Ethereum, Polygon.
Development state:	*Testing, demo scheduling.*

Quadrata is a project that is still in testing phases. There isn't that much information available on the exact mechanics behind their on-chain ID, but we wanted to include it nonetheless. The project is incubated/developed by Spring Labs, a company focused on the protection of business data through the use of blockchain technology.

Quadrata offers the ability to mint on-chain ID in the form of non-transferrable NFTs. These are reminiscent of Soul Bound Tokens that are tied to one wallet and are not able to leave that wallet. These kinds of tokens have the ability to shape characteristics and identity to that wallet by assigning specific traits or information to the non-transferrable NFT. Passport holders have the ability to burn their Quadrata passports with the *QuadPassport.burnPassports()* function.

That is exactly what Quadrata aims to provide. Characteristics vary from an Anti-Money Laundering (AML) score to Country and wallet information. These characteristics help other protocols and projects gauge the trustworthiness of the wallet they are dealing with and to stimulate adoption of the on-chain passport, Quadrata has published a lot of guidance on integrating their code and passports into other protocols. Every time a Quadrata attribute is queried on-chain, the protocol charges a query fee, which on mainnet varies between $0.00012\ ETH\ to\ 0.015\ ETH$ and on Polygon between $1.2\ and\ 15\ MATIC.$

As of writing, Quadrata is still testing out their product and little information is disclosed on the exact scoring of AML risk. Quadrata is backed by *Dragonfly Capital, Franklin Templeton, Abra, GSR Ventures, Orange DAO, Fellows.fund, Greatpoint, AugustCapital, and QuantStamp.*

Pros	Cons
Uses TrueZero Tokenization, a new technology to protect data.	No documentation for further details.
	The Query fee they charge can result in being

	very high.

Tech applications - Machine Learning, Proprietary Oracles and Index Data

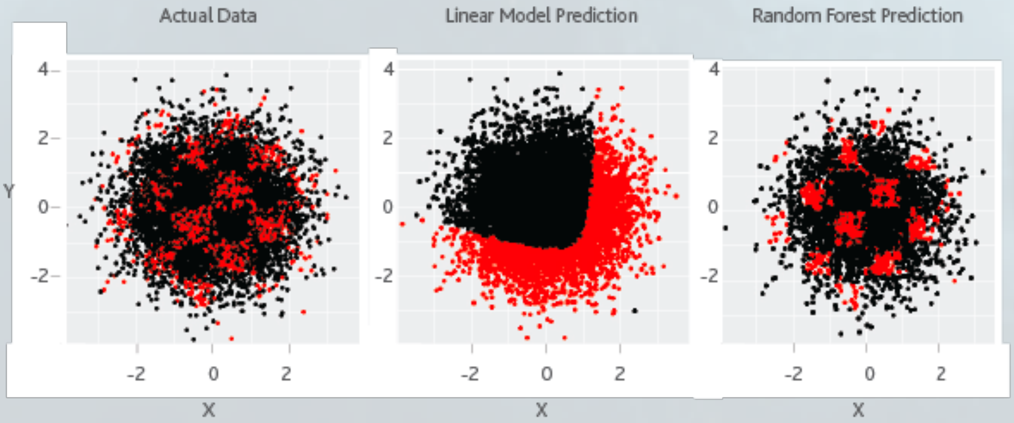
Using Machine Learning (*ML*) for credit rating could push DeFi into credit modeling and could end up in representing a huge competitive advantage for protocols that adopt such technology.
Its main benefits are:

- the ability to fetch, scan, categorize and interpret large datasets on different chains;
- the creation of virtuous cycles since the prediction products and their underlying architecture tend to create a loop where more data leads to better products, which lead to more users and in turn, more data.

Drawbacks of using ML are that sometimes the results produced by these methods can be difficult to interpret, but these methods provide a better fit for the nonlinear relationships between the explanatory variables and default risk. We also find that using a broader set of variables to predict defaults greatly improves the accuracy ratio, regardless of the models used. ML is already used by Moody's, one of the leading TradFi credit rating firms, in their Analytics RiskCalc model that they use as the benchmark model for rating.

Machine learning can result in being more accurate than statistical modeling, as typically statistical learning methods assume formal relationships between variables in the form of mathematical equations, while machine learning methods can learn from data without requiring any rules-based programming, thus being more flexible.

Let's consider this example for better understanding;



Source: Moody's Analytics

The first chart shows the actual distribution of data points with respect to $X \, and \, Y$, while the points in red are classified as defaults. This can be related to a geographical map, where the X axis is longitude, and the Y axis latitude.

Let’s consider the areas in red to represent high-risk demographics, with a higher default rate. As expected, a linear statistical model cannot fit this complex non-linear and non-monotonic behavior. If we use the *random forest model*, a widely used machine learning method, this turns out to be flexible enough to identify the hot spots since it is not limited to predicting linear or continuous relationships. Most of the machine learning models, unconstrained by some of the assumptions of classic statistical models, can yield much better insights that a human analyst could not infer from the data. At times, the prediction contrasts starkly with traditional models.

A complete ML credit rating system should include three different algorithms: artificial neural networks, random forest, and boosting. While in TradFi the performance of such algorithms is guaranteed by the availability of doxxed information and transparent statements, the use of ML and AI in DeFi must be designed in a whole another way, taking into consideration on-chain analysis and volume metrics.

Particularly fit for the prediction of defaults is *lasso regression*. Lasso regression is a regularization technique standing for Least Absolute Shrinkage and Selection Operator. It is used over regression methods for a more accurate prediction using shrinkage. Shrinkage is where data values are shrunk towards a central point as the mean. The lasso procedure encourages simple and sparse models (i.e. models with fewer parameters). In TradFi, the credit scoring model is treated as a kind of statistical model which analyzes a large amount of customers’ historical data and extracts the laws and features of credit risk. Then an appropriate model is constructed to evaluate the risk for new applicants or existing customers. While this seems to be a working method to handle scoring and rating, also logistic regression performs better in prediction accuracy and seizing key factors that impact credit risk, compared with the full model and stepwise regression; even though it may perform badly when levels of a categorical variable are coded as a collection of binary covariates.

Proprietary oracles

Proprietary oracles can provide comprehensive and dynamic credit ratings for users through an oracle node network that enables off-chain credit calculation with the results fed on-chain into smart contracts. This can be done through the W3C standard compliant DID protocol, establishing the modeling for participants’ public historic cross-chain data by constructing an oracle network and a trusted computing element network.

When a smart contract on the blockchain needs to obtain specific data, it would send a data request to an oracle(‘contract request’). The protocol’s oracle would then register the data request as an "event" and send the data request to the corresponding nodes, starting the validation bidding process among the different nodes. The oracle would select a certain number of appropriate oracle nodes to complete the task. The nodes selected by the credit oracle would obtain all the data and provide a result after verifying and aggregating this data.

Furthermore, an own oracle allows developers to securely connect smart contracts to trusted, tamper-proof analytics products created using on-chain and off-chain data streams.

Both of these options seem to be something teams are working on and haven't gotten that much adoption so far due to the technical difficulties involved in their implementation.

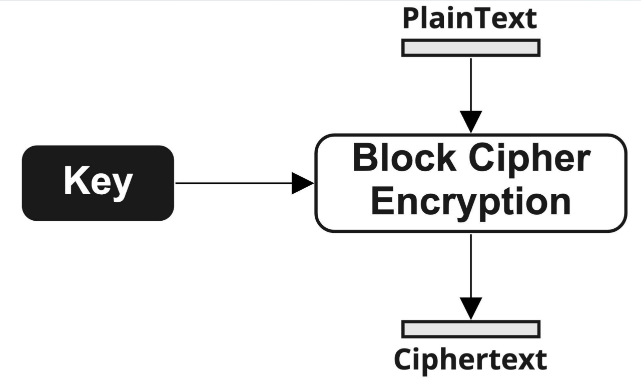
Functional and fully homomorphic encryption

The vast majority of financial organizations that manage confidential data are well aware of the security threats of the existing solutions and leverage solutions such as storage encryption, transport-level encryption, and intrusion detection systems. However, these measures do not address threats posed on the *data-in-use*. Among the preferred approaches for mitigating these threads are Homomorphic Encryption (HE) and hardware-assisted Trusted Execution Environment (TEE).

An example of secure financial computation is Credora Inc. They combine Intel SGX TEE technology and HE based Zero Knowledge Proofs to shield customers' data against malicious actors. By relying on hardware infrastructure, this combination is constrained by having to trust Intel and the SGX, even if we assume the manufacturer to have an interest in producing reliable hardware.

Credit scoring fits splendidly with the emerging cryptographic scheme of *Functional Encryption (FE)*, which allows a user to only learn a function of the encrypted data. In a FE model, there are special evaluation keys that exclusively allow the functional evaluation of encoded data.

FE enables selective access control of sensitive data d basing on specific functions $f(d)$. In an FE scheme, a decoding key $sfKey(f)$ is associated with the function f. Therefore, the decryption of an encrypted data d through $sfKey(f)$, provides the function evaluation $f(d)$, and nothing more about d.



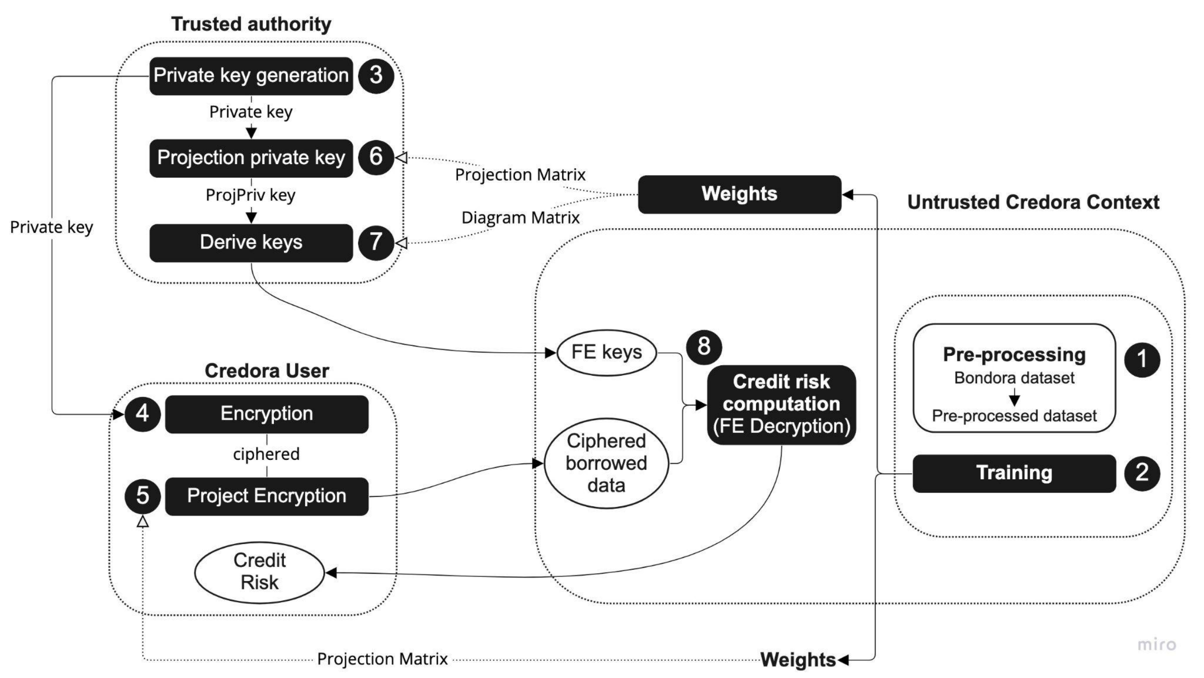
Funcial Encryption framework

Fully homomorphic encryption is a scheme that enables analytical functions to be run directly on encrypted data while yielding those encrypted results as if the functions were on plaintext. This solution has the benefits of:

a) not having any trusted third-party, meaning that the data remains encrypted at all times;
b) eliminating the tradeoff between data usability and data privacy, as there's no need to mask/drop any features in order to preserve the privacy of data;
c) quantum-safe, as FHE schemes are resilient against quantum attacks.

This ultimately comes at the cost of a poor performance due to slow computation speed and accuracy problems. It can be extracted that FHE remains feasible for computationally simple applications.

Concerning are the differences between FE and FHE. On the one hand their results are similar because once the message has been encrypted, both evaluate a function of the message. However, FHE suffers from the additional step of decrypting the evaluation of the function, since the result of its computation is still an encrypted result.
With FE alternatively, the result of the decryption already represents the evaluation of the function.



Credit Scoring through FE architecture

An additional advantage given by the FE scheme is that it enables *Attribute-based encryption* (*ABE)* schemes, where the encrypted data is linked with a set of attributes and secret keys along with certain policies that allow the controlling of ciphertexts which can be decrypted depending on the possessed attributes. Concluding on FE, we can state that it tries to change this paradigm by allowing more fine-grained access to encrypted data and improving its flexibility.

Bird

Bird.Money	
Website URL:	*https://bird.money/*
Chain(s):	*Binance Chain, Solana.*
Token:	*$BIRD.*

Bird Money provides an on-chain credit score by using machine learning. Their credit score is dubbed *Blockchain Individualized Risk of Default Score* (*BIRD*) and assigns three types of scores: unknown risk, low risk and high risk.

The platform combines machine learning with on-chain and off-chain data sources to differentiate borrowers' default risk. The model BIRD uses is adverse selection and predictive analysis based on extensive data curation and statistics. Bird's proprietary data lake takes into consideration individual wallets data, wallet network analysis, digital off.chain data (social media, web history), and other off-chain data (employment, TradFi accounts). This data is then run through an artificial neural network to then be scored.

The platform includes a native token, $BIRD, that must be used to pay transaction fees and to leverage CCTS scores. The token has a max supply of 140,000 with more than 70% of the supply already burnt. Allocation is allegedly not disclosed.

Additionally, an analytics oracle is used to allow users to retrieve data from the Bird team, like proprietary credit ratings and important real-world events. The oracle analyzes users' account activity, payment history, and other important loan metrics.

Bird has partnered to integrate their services with *API3, CyberFi, UniWhales, MoonTools, unmarshal, Glitch, Parsiq, and DeFi Pie.*

The team is composed of 24 people, fully doxxed, and with huge experience in Web2 fintech companies.

Pros	Cons
Ability to offer native on-chain scoring.	Exact details on mechanics are missing.

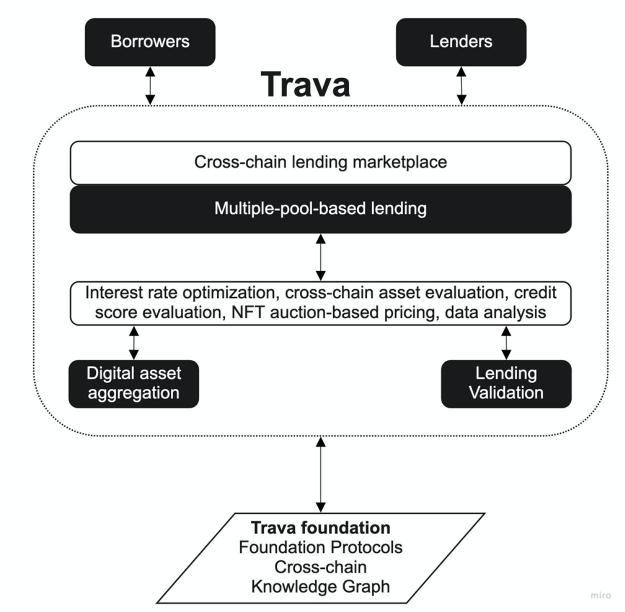
	Incomplete docs on credit rating.

Trava

Website URL:	*https://scoring.trava.finance/*
Chain:	*BNB Chain.*

Trava Finance aims to become a lending marketplace for anyone. The protocol allows users to become pool owners, who create and manage their own lending pools. Pool owners are in the position to increase their earnings by successfully setting the right interest rates and attracting borrowers and lenders to their pools.

Another considerate pillar to Trava is their cross-chain data analysis, marked as "semantic knowledge graph", that is used to recommend optimal pool parameters to pool owners, detect unusual activity in the lending pools, and evaluate credit scores of users. These scores can be used by pool owners to reduce lending risk as they are able to set credit-score thresholds and prohibit users with bad lending history from entering the pool. Additionally, pool owners are able to stimulate borrowing in their pool by allowing higher credit score wallets to take out higher LTV loans.


Borrowers
Lenders
Trava
Cross-chain lending marketplace
Multiple-pool-based lending
Interest rate optimization, cross-chain asset evaluation, credit score evaluation, NFT auction-based pricing, data analysis
Digital asset aggregation
Lending Validation
Trava foundation
Foundation Protocols
Cross-chain
Knowledge Graph
miro

Trava architecture

Data from multiple chains is used for wallet identification and scoring, although it is not made clear which chains specifically besides Ethereum. Trava claims to aggregate and analyze all transactional data from the chains to conduct a credit score. The score is mostly based on historic lending activities and the trustworthiness of tokens measured by market capitalization, volume, and transactions. Higher scoring tokens result in a higher credit score.

More precisely, the following areas are taken into account:

a) **Total assets** - easures the total financial strength of the users' wallet(s). It is calculated by the sum of current balance and investment minus liabilities. Users with higher total financial strength will receive a higher scoring;
b) **Transaction history** - aggregates transactions on exchanges, regarding loans and deposits across multiple dApps. The score is derived from multiple sub-parameters, such as age of the wallet, transaction count, frequency of transactions, number of liquidations, and total value of liquidations;
c) **Loan ratios** - represent the debt ratio of the account;
d) **Circulating assets** - represent how active the owner of the wallet(s) is. The more money he has invested, the higher his creditworthiness is estimated to be. The score is derived on two sub-parameters: Investment-to-total-assets and Return on Equity;
e) **Trustworthiness of balance asset** - if the user holds a basket of trusted blue-chip tokens, his credit score is estimated to be higher.

The computed credit score is useful to pool owners, because they are able to:
a) reduce the lending risks by defining a credit-score threshold for borrowers participating in the lending pool; and b) stimulate borrowing by defining a high LTV ratio for borrowers with high credit scores.

Trava also offers cross-chain identification, a feature that is employed to verify that multiple addresses on different chains belong to the same user. This is managed through a wallet application where users can manage their accounts and prove ownership of their addresses. A small fee is charged for transactions that activate the cross-chain identification protocol.

To expand their product offering, the protocol developed an auction-based pricing model for NFTs. Trava hosts an auction after which a borrower can use the auctioned NFT as collateral. The process works as follows: a) the NFT holder opens the auction session setting the parameters used; b) users interested in the NFT can join and are incentivised to do so by liquidity mining; c) depending the format of the auction, either auction-to-sell or auction-for-buy-right, the auction concludes.

The Trava token is the utility and liquidity mining token of the protocol, and it is currently hosted on the Binance Chain. The project has been partnered with *Router, Kawaii islands, Dfyn, Nest, TechFi, Chainlink, Chainstack, and Oraichain.* The platform has been audited by *Hacken* and *Certik*, where four major issues were found and are currently unresolved.

Pros	**Cons**
Next to credit rating, Trava facilitates lending, so there is an immediate use case.	Only conducts a score based on the wallet.
Takes into account various metrics to conduct a score. The analysis is broad.	Some metrics are questionable, like trustworthiness of certain assets.
	Docs filled with a bunch of buzzwords.
	Certik's audit reports 4 major vulnerabilities still unresolved.

Zk-KYC

The use of zero-knowledge proofs in know-your-customer practices fits DeFi credit rating needs best. ZkKYC is a solution concept for KYC without knowing the customer while leveraging self-sovereign identity and privacy. It is a form of KYC that does not rely on upfront sharing of personal information with the counterparty/business, but still enables the identification of the customer if required.

In current KYC practices, when onboarding on a business a user must present their ID, the business then verifies the ID with a third-party identity verification service and if the identity is successfully verified, the user becomes a customer.

The zero-knowledge solution takes into account the creation of a ***Token*** that has to be generated by a potential customer and contains an identifier with verifiable information. The *Verifier*, i.e. the business, cannot read the information inside the token but is able to verify that the token contains the correct information. This is a highly desirable solution for both the customer and the verifier as the process takes place in a completely trustless and seamless manner. It has the potential to reduce process time and costs significantly by handling it on-chain.

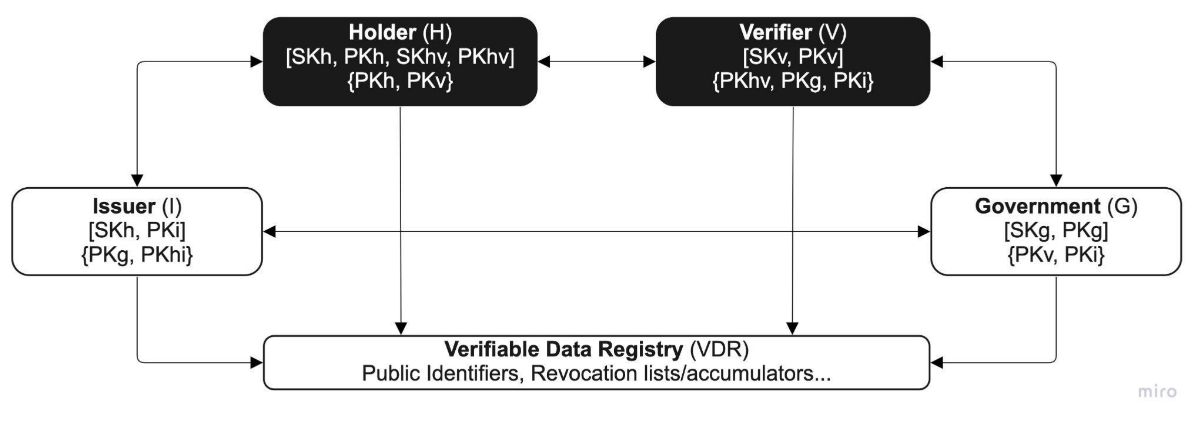
A Verifier under zkKYC can request the *Holder* (customer) to present three types of information:

- **Eligibility proof**: proof that the Holder meets the (business) criteria set out to be able to provide access to their service;
- **zkKYC token**: encrypted data object that contains information to enable the Holder's identity to be revealed to specific parties only;
- **Validity proof**: proof that the presented zkKYC token contains the correct information, without disclosing what that information is.

The objective definitely is improving security and privacy by taking away the need for businesses/merchants to have to process and store sensitive customer information.

This whole concept is based on the pillars of

- **Self-Sovereign Identity** (*SSI*): digital identity documents can be held in a personal digital wallet. The user becomes a holder and he can present his documents to verifiers when requested;
- **Decentralised Identifiers** (*DID*): they can identify any subject (did: did method: did method specific identifier). The string allows a specific resolver to resolve a specific DID document from a Verifiable Data Registry;
- **Verifiable Credentials** (*VC*): issuers issue a VC to a Holder and digitally sign it with the secret key associated with their DID.



zkKYC Concept Overview, Chainlink labs

Cryptographic signatures enable the holder to generate zero-knowledge proofs (ZKP) for a verifier. Users have the ability to reveal only a selected set of attributes while hiding everything else and prove that something is true/false/greater/equal without giving up specific, sensitive information or revoking credentials.

Instead of the public-blockchain compute cycle that is:

$$propose \rightarrow validate \rightarrow transact,$$

the cycle on privacy-oriented blockchains features point-to-point encryption of addresses and amounts, to shield every users’ broader subgraph:

$$propose \rightarrow encrypt \rightarrow validate \rightarrow encrypt \rightarrow transact.$$

Under this structure, the validators themselves don’t know what they’re validating, they just know (via zero knowledge) that what they are verifying is, in fact, an agreed transaction between an unknown sender and receiver for an unknown but mutually agreed amount; only the sender and receiver know the actual amount transacted or smart contract executed.

A chain that would best suit the creation of zkKYC is the Cosmos IBC’s Secret Network. A thing to keep in mind when considering building on Secret is that, to open-source developers, Secret represents a big shift in complexity without (yet) corresponding demand.

For user adoption, it is considerably important to consider making zkKYC a cross-protocol feature allowing users to input their data once and interact with protocols seamlessly. For this particular point, *KYC_protocol_A* and *KYC_protocol_B* might do very different processes for each individual going through zkKYC, thus every protocol needs to be familiar with the issuers' procedures for zkKYC'ing. Since KYC usually needs to be refreshed at least once every 12 months, protocols need to find a way to "remove" KYC'd status from an individual address and/or “update” it.

The zero-knowledge technologies aren't risk-free either, as per our research there persist two important issues:

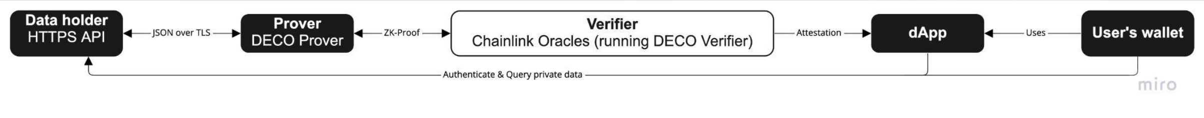
- **No entire guarantee** - even if the probability of verification by the verifier, while the prover is lying, can be significantly low, ZKPs don't guarantee that the claim is 100% valid. The probability of a prover lying decreases in each iteration of the ball-picking process, but it can never reach zero. Thus, zero-knowledge proofs aren't actual proofs in a mathematical sense;
- **Computation intensity** - algorithms used are computationally intense as they require many interactions between the verifier and the prover (in interactive ZKPs), or require a lot of computational capabilities (in non-interactive ZKPs). This makes ZKPs unsuitable for slow or mobile devices.

Chainlink's DECO

Decentralized oracle (*DECO*) is a privacy preserving oracle developed by Chainlink, a leading researcher in the field of zkKYC. DECO allows users to prove that a piece of data accessed via transport layer security (*TLS*) came from a particular source and optionally prove statements about such data in zero-knowledge, keeping the data secret. It is the first solution that works without hardware and server-side modifications.

The development stems from the power of TLS, which is a widely deployed protocol that allows users to access web data over confidential, integrity-protected channels, but that has a serious limitation: it doesn't allow a user to prove to third parties that a piece of data she has accessed authentically came from a particular website.

DECO is therefore a mechanism that allows users to export any data they have access to enabling a whole new attire of currently unrealizable applications. The oracle is source-agnostic and supports any website running standard TLS enabling anyone to become an oracle for any website.
At a high level, the prover entrusts a piece of data *(D*) and proves to the verifier that D came from a TLS server (*S*) and optionally a statement (*πD*) about D. At a low level DECO achieves authenticity with the verifier being convinced only if the asserted statement about D is true and D is indeed obtained from website S.



DECO's use of zero-knowledge proofs, Chainlink Research

Three primitive use cases were given by Chainlink: a) a confidentiality-preserving financial instrument using smart contracts; b) converting legacy credentials to anonymous credentials; and c) verifiable claims against price discrimination. These examples reflect the high efficiency of DECO.

Protocol own chain

Another way of performing credit rating is by constructing a whole chain for this purpose. This approach is reminiscent of the 2017 era during which projects applied blockchain technology to every data(base) reliant problem users could think of. The obvious motive for this approach is a global, decentralized solution that is transparent and fair for any participants.

This kind of solution is adopted by *Masa Finance, Bloom,* and *Krebit* among others. That being said, all three projects are struggling to find adoption. Compared to other previously discussed solutions that run on top of an already existing L1, it seems that there is no direct benefit in having a separate chain without the solution having any demonstrated traction. If the 'credit rating'-L1 were to use zero-knowledge proofs, it could result in an easier integration with privacy-preserving features.

Most of the solutions on the market are geth forks that try to make sure to protect sensitive financial and credit data. This can also help to enhance the security of a credit rating process, because normally the interaction between a blockchain and the outside world is usually conducted by distributed ledger technology oracles. This implies that data from outside a blockchain, also referred to as off-chain data, cannot have the same level of trust as data originated from the chain (on-chain data). A way to make credit computation trustworthy is to conduct it on-chain, and doing so on determinate existing blockchain can result in the process being resource-consuming and/or time-consuming.

Having a native chain can result in more friction of getting access to capital coming from: a) users not wanting to get exposure to new bridges, b) users not wanting to dilute their capital in different chains and c) users not wanting to use a potentially centralized blockchain. A clear risk for this type of solution stands in bridges, which are indeed necessary if a protocol decides to create its own chain. Besides bridges, the development and implementation of native L1 technology can be costly and time-consuming while the benefits coming from having adopted this approach can be outsourced to other more trusted chains.

Bloom

Bloom	
Website URL:	*https://bloom.co/*
Token:	*$BLT.*

Bloom protocol is a decentralized credit scoring system on Ethereum powered by IPFS. They assess credit risk through federated attestation-based identity verification and credit staking.

The Bloom Protocol is composed of three main systems: a) BloomID – which is an identity attestation, b) BloomIQ – which is a credit registry; and c) Bloom Score – which is a credit scoring system.

Bloom Network aims to provide credit scoring through federated attestation-based verification and the creation of a global credit scoring. The main motive is to solve cross-border credit scoring and to create a competitive credit scoring market. Currently, credit scoring is often done locally and in the hands of a small number of entities. This is done through BloomID, which lets users establish a global and federated identity with independent third parties who publicly vouch for their identity information and creditworthiness. These third parties usually are organizations who earn revenue by evaluating a user's credentials.

BloomScore relies on peer-to-peer credit stakes from BloomID using an user's spending habits and credit activity as a proxy for creditworthiness. The goal of the Bloom network is to expose securely encrypted information about financial networks and historical payments so that both lenders and borrowers benefit.

Bloom focuses on creating a decentralized, global network that provides credit scores, rather than bringing credit scoring to on-chain. Their goal is to have existing organizations transfer users' history and scores over to the network and connect that data to the users' BloomID, their online identity. Bloom's network relies on peer-to-peer credit stakes for trustworthiness. The main idea is that people are able to vouch for one another if the right incentives are in place. By allowing users to stake in the system and attest to others' creditworthiness, a system of trust is built that is able to facilitate accurate credit attention.

The creditworthiness check on bloom is called reliability score and is a prediction of whether a user is likely to pay back a future loan on time given their past financial activity. It takes in consideration the total amount paid versus total amount owed, the longest repayment history on file, the average payment total per month, the number of past loans, and the total amount paid across all reported data. The scoring phases is divided in three phases:

In the first scoring phase, given these indicators, Bloomcalculates a multivariate logistic regression in which the indicators are represented as vectors $x \ = \ (x_1, x_2, x_3, x_4, x_5)$ and will also have a corresponding weight such that the logit is $g(x) \ = \ \beta_0 + \ \beta_1 x_1 \ + \ \beta_2 x_2 + \ldots + \beta_5 x_5$ and the regression is expressed by:

$$\mathrm{R(u)}=\frac{e^{g(u)}}{1+e^{g(u)}}$$

Where β_0 is an offset, β_i is the weight for the x_i indicator and u is a user of the network. The transformation of the continuous indicators into discrete values requires adding dummy variables for each indicator. The final calculated score is scaled up and between 0 and 100. Weights, indicators, and categories are subject to a vote on the bloom network.

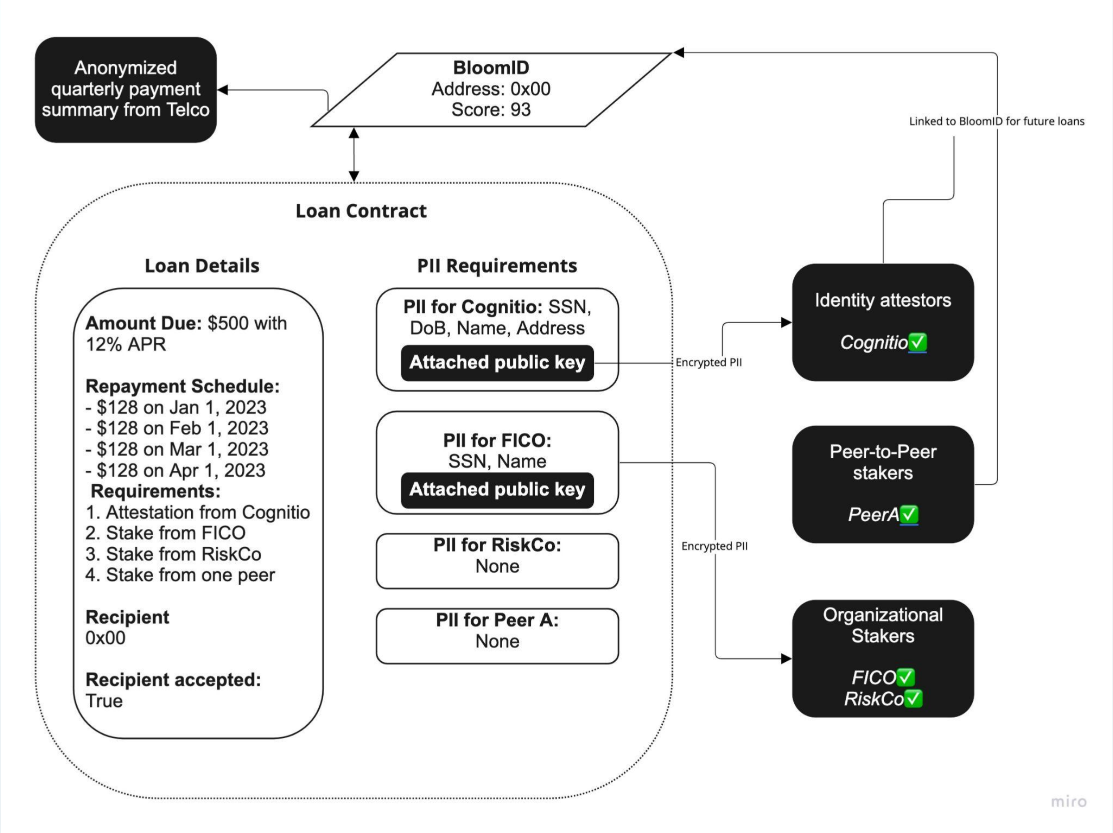
After the first scoring phase, the peer score of a user will be the average score of each peer that the user has staked to and is capped at a maximum of 50 and represented by the equation below, where s stands for the number of peers that a user has staked.

$$min(50, \textstyle\sum_{i=0}^{s} \quad \frac{R(u_i)}{s})$$

After this second scoring phase, the final phase of account maturity begins and the user has their own financial activity complete. The Bloom score is subsequently uncapped. The score will be calculated with the following equation, where P corresponds to “paid”, and T to “total owed”.

$$\sum_{i=0}^{s} \ \frac{R(u_i)}{s+n} + \sum_{j=0}^{n} \ \frac{P_j/T_j}{s+n}$$

To sum things up, in the graph below is a full risk assessment lifecycle on Bloom that includes one attester and three credit stakers.



Pros	Cons
A global, decentralized solution for something that is often done locally and in the hands of a small number of entities.	They are currently investigated by the SEC for their ICO and threatened by a $31mln fine if not compliant.
The division of the credit scoring in three different phases with scoring caps protects the protocol from some malicious attacks.	Not detailed whether sensitive users' details are shared on-chain and privacy is guaranteed.
Peer-to-peer network that is beneficial to the collective.	Requires active participation from retail in order to work properly.

Masa

masa	
Website URL:	https://www.masa.finance
Chain(s):	*Own L1 Blockchain (testnet).*
Token:	*$CORN.*

Masa is both a hybrid credit protocol and a decentralized credit bureau. They have launched a Personal Finance Management Platform (*PFM*) that aggregates users' on-chain and off-chain data and behavior by minting a non-fungible credit report. Users are able to access credit based on their report.

The protocol has a native token, $CORN, which is used for governance, as a utility token, and as reward paid out to liquidity providers. In this last case, the interest on loans is collected in USDC and converted into CORN before being paid out to LPs.

The protocol is a *Proof-of-Stake* (*PoS*) blockchain built on a forked version of geth. They use the *Tessera transaction manager* to provide zero-knowledge private transactions and private smart contracts that can be used for transacting sensitive financial and credit data. Masa achieves transaction privacy by a) enabling transaction submitters to create private transactions by marking who is privy to a transaction via the *privateFor* parameter, b) storing encrypted data off-chain, and c) replacing the payload of a private transaction with a key for the location of the encrypted payload, such that the original payload isn't visible to participants who aren't privy to the transaction. Note that the protocol does not intend to create new types of transactions but only to extend Ethereum transaction models to include an optional parameter. This way,

- **private transactions** have payloads visible only to the network participants who have their public keys specified in the *privateFor* parameter of the transaction, which can take multiple addresses in its list;
- **public transactions** have payloads visible to all participants of the same network and are standard Ethereum transactions.

Private transactions are executed differently from the standard ones as before, because the sender's Masa node propagates the transaction to the rest of the network, then the node substitutes the original transaction payload with a key for the location of the encrypted payload received from Tessera. Participants privy can replace the hash with the original payload while not privies only see the hash. In addition to standard privacy (*SP*), Masa enhances privacy by introducing Counter-party protection (*PP*), Mandatory party protection (*MPP*), and Private state validation (*PSV*).

On June 1st of 2022, Masa announced the second phase of its testnet. The first and second phase are all about bootstrapping validators and running the network. Both phases are incentivized, but mainly aimed for the more tech savvy crypto users who run validator nodes. The second test phase is expected to last around six to eight months. Upon mainnet, the protocol plans to set up bridges to Ethereum mainnet and Celo network.

Important to note is that not all of Masa’s products are available everywhere, as some services are only available in determined countries. Masa has a bunch of backers and partners including CitizenX, Celo, Goldfinch, GSR ventures, Intersect VC, EQ, Unshackled ventures, Ledn, Flori Ventures, Lateral capital, and GoldenTree Asset Management.

Pros	Cons
Creating non-fungible credit reports for users.	Incomplete documentation.
Working with 10k off-chain data sources and integrating with exchanges and wallets.	Lenders are only “trusted”.
“Hybrid model” instead of a full decentralized model for closing partnerships.	Completed a pre-seed round in June 2022, strongly reliant on VC funding.
Founder is a former TradFi CEO, as he ran a company that conceded API to Banks and Fintechs.	

Krebit

Website URL:	https://krebit.id/
Chain(s):	*Ceramic Protocol, Polygon.*
Development status:	*Beta.*
Token:	*$KRB.*

Krebit allows users to take control over their data in the form of digital identities and are marketing their product as a *reputation passport* that allows users are able to prove things about them without revealing unnecessary information. Their solution addresses the challenges of Decentralized Reputation (DeRep) of sovereign-identities, reputation calculation, sybil attacks and vote apathy creating a pseudonymous economy for users to prove things about them without revealing any unnecessary information. The digital identities are created on top of *Ceramic Protocol*, a data-focused blockchain that enables dApps to manage content. Other projects built on top of Ceramic are *Enigma, Origin Protocol,* and *Streamr.* Krebit takes advantage of Ceramic's sign in with ethereum (*SIWE*) decentralized identity (*DID*) for login with a non-custodial wallet.

Via Krebit users can claim data which can be anything from their location and identity to their social media accounts. The claim data is then stored off-chain and encrypted on the Ceramic network. Verifiers are the validators of Krebit that verify certain claim data upon request and send an attestation back to the issuer. The framework of the process starts with users managing their claim information and then requesting a judgment from a verifier/provider based on a fee that they are willing to pay. At this point a verifier with enough $KRB tokens validates the data, signs the Verifiable Credential, and sends the attestation back to the user. Both users and issuers are rewarded at the end of this process when credentials are registered on-chain with liquidity mining rewards. As credentials can be issued, they can also be revoked, suspended, deleted, expired or disputed.

To dispute a Verifiable Credential, any member can submit a proposal to the Krebit DAO and if the proposal goes through, the $KRB rewards would get burnt and the verifier's stake could get slashed. While this seems to be a functioning system at its current size, we believe that the approach may have to change if Krebit gains mainstream traction.

Krebit is now focussing on building a reputation in the DID and making it more appealing to the job industry and recruiters to find reputable future employees in a decentralized manner. Verifications made by Issuers about off-chain claims are stored in Ceramic and registered on-chain in the KRB Ethereum token. The Krebit team has recently extended the capabilities of the passport to be able to stamp credentials associated to a) personhood (discord, twitter, email, phone, KYC…), b) work experience (spect, dework, github…), and c) education and community. These credentials can be verified on-chain with krebit-contracts in the polygon network while the users' private data is both hashed and encrypted using the Lit protocol.

For offering their product Krebit uses EIP712-VC tools, based on the W3C Ethereum EIP712 Signature 2021 Draft. Such approach provides functions for creating off-chain Verifiable Credentials in Ceramic that can be verified on-chain with krebit contracts.

Pros	Cons
They offer a passport model that could be used mainly in human resources but that can be expanded in credit rating.	Documentation not available as for writing.
Can become an infrastructure layer for dApps using the protocol to conduct decentralized KYC/AML, restrict access to Adult/NSFW pages and prevent anti-Sybil.	Very few use cases as of writing.
The team is well aware of the importance of privacy for users and recently implemented zkEVM features using Lit protocol.	

Risk and Threats

We have divided this paper into a few sections dedicated to specific on-chain credit rating solutions. The aim of this section is to suggest a framework on responses and dynamics to deliver a credit rating service. In the end, they all boil down to the trade-off between performing traditional KYC or enforcing trust on code level. The former being reliant, but centralized, the latter being decentralized, but complex and prone to manipulation. To visualize, we thought it would be best to end with a table containing risks and threats to these approaches.

Solution	Risks and threats
Traditional KYC practices	● Potentially giving up sensitive information; ● At the moment only scalable to a certain degree and only practically deployed for institutions; ● Slowdown of the loan approval process.
NFCs that bundle wallet activity and compute score	● Need to constantly be fed with new data to stay up to date which is gas consuming; ● Prone to manipulation; ● Impossible to ensure all wallets of users are captured, also not desirable as it breaches privacy; ● Hard to punish bad behavior as there is a lack of legal enforcement.
Social recourse to enforce repayments	● In a pseudo-anonymous world, social recourse is ineffective.
Credit scoring based on attestations	● Requires a lot of user input thus being time consuming; ● Likely hard for most to gather attestations.

Conclusion

The transparent nature of distributed ledger technologies provides the system with a lot of easily accessible data that could help the credit rating industry to give more complete ratings compared to the TradFi world. The main challenges in performing credit rating are embedded directly in the nature of the system itself, as pseudonymity and the possibility to create a number of wallets can represent a threat in screening a past user behaviour.

When it comes to the business version of DeFi, this being DAOs and protocols, the rating procedure becomes increasingly difficult. Liquidity mining and incentives can trick the rating process in the suitability of the business model making it really hard to implement a framework to break down product-market fits.

In this paper, various solutions to credit rating were highlighted and each comes with its own set of trade-offs and risks. It all boils down to enforcing trust in a pseudo-anonymous, digital world which has proven to be a hard and complex challenge. The solution that comes the closest is presented by Credora. Although the protocol right now is to a degree fairly centralized, it is imaginable that in the future once it has established a large network of participants, the protocol will be able to decentralize and host their own network. The foundation is laid in the form of infrastructure that performs credit scoring of institutions while also protecting sensitive data using zero-knowledge technology. Credora's solution is one that comes the closest to true KYC.

A wide variety of other projects focus on bringing credit rating to individual users by collecting on-chain wallet data and performing some form of scoring models on it. The main problem in this case is the fact that users can hide wallets from the protocol and by doing so, manipulate their score. It is impossible for protocols to capture all the wallet data from users and should also not be desired. This violates to some extent the privacy of the user, who, understandably so, does not want to give up all his/her wallet addresses. Another issue here is that some of these protocols only bundle and use lending history and derive their scores solely from that data. This neglects other key factors, like participating in rugs and questionable projects.

In absence of an on-chain KYC method, trust has to be enforced on code level. Let it be using machine learning to calculate scores or bundling on-chain transactional history in an NFT. Each comes with its own pitfalls and currently the question remains whether these solutions are fit for the web3 world. A lot of projects struggle with enforcement and therefore the more successful ones rely on KYC and legal oversight to ensure that the borrowers are healthy and trustworthy.

While on-chain analysis, zkKYC, machine learning, having an own chain/oracle, and NFCs can apport lots of data and info, the most suitable product on the market seems to be the one offered by Credora. An increasing number of protocols is deciding to have a third-party assess the risk associated with giving out a loan, having then the possibility to a) use a functioning framework and b) focus on development. Given the trustless, permissionless and autonomous nature of the ecosystem, we consider that machine learning can go along with the industry standards but implementing such a solution can be costly in terms of research and workforce.

The harsh reality is that, often, a credit score is merely a snapshot of the entities' creditworthiness at a given moment. This is the case for NFCs that bundle and process the data of certain addresses, but it seems that for Credora it is also the case. As Crypto Condom points out on Twitter, Wintermute still is categorized with an A despite being in distress. This is the case across a few protocols they are connected to and shows that a real-time solution would be highly desirable.

The nature of DeFi creates a whole different scale of risks that make it worth it to be separated to the TradFi's one. As one of the space's blue-chips, Compound was rated by a major traditional credit rating firm as "junk" because of the use of stablecoin in their services, it seems pretty clear that a different approach must be taken in decentralized finance.

Bibliography

Dinesh Bacham and Janet Zhao, “Machine Learning: Challenges, Lessons, and Opportunities in Credit Risk Modeling”, *Moody’s Analytics* (July, 2017). https://www.moodysanalytics.com/risk-perspectives-magazine/managing-disruption/spotlight/machine-learning-challenges-lessons-and-opportunities-in-credit-risk-modeling

Krebit, “Decentralized Reputation (DeRep) for a Web3 of Trust”, Yellow Paper (August, 2022). https://ipfs.io/ipfs/QmacmL7Dwh1gW6ksyheyQwgGf6oDLoYPUgev5LKDt8xcXU?filename=Krebit%20YellowPaper%20v0.3.pdf

Ceramic Network Documentation (August 2022). https://developers.ceramic.network/learn/welcome/

Hongmei Chena and Yaoxin Xianga, “The Study of Credit Scoring Model Based on Group Lasso”, School of Statistics, Capital University of Economics and Business, Beijing, China, (2017) https://pdf.sciencedirectassets.com/280203/

“Functional Encryption”, Wikipedia, (September 18, 2022) https://en.wikipedia.org/wiki/Functional_encryption

University of Naples ’Parthenope’, Department of Engineering × Credora Inc, “Privacy-preserving Credit Scoring via Functional Encryption”, Research Paper, (September 22, 2021) https://arxiv.org/pdf/2109.10606.pdf

Cornell University, “Scoring Aave accounts for creditworthiness”, Research paper (September 18, 2022)
https://arxiv.org/abs/2207.07008

Credora Documentation (September 2022). https://credora.io/about/

Cred Protocol Documentation (September 2022). https://docs.credprotocol.com/

Teller Finance Documentation (September 2022). https://teller-hosting.s3-us-west-1.amazonaws.com/Teller+Protocol+V1.0+Whitepaper.pdf

Spectral Finance Documentation (September 2022). https://docs.spectral.finance/

RociFi Documentation (September 2022). https://docs.roci.fi/

CreDA Documentation (September 2022). https://creda-app.gitbook.io/creda-protocol/introduction/creda-protocol-whitepaper

AlphaWallet Documentation (September 2022). https://alphawallet.com/

Solv Protocol Documentation (September 2022). https://docs.solv.finance/solv-documentation/

Bird Documentation (September 2022). https://docs.bird.money/

LedgerScore Documentation (September 2022). https://docsend.com/view/vyuwhy6i7dcegyk6

Bloom Documentation (September 2022). https://bloom.co/documentation/

Masa Finance Documentation (September 2022). https://developers.masa.finance/docs

Deco, Liberating Web Data Using Decentralized Oracles for TLS, extended version, Chainlink Research (September 2022). https://research.chain.link/deco.pdf

ARCx Documentation (October 2022). https://wiki.arcx.money/welcome/arcx-credit-introduction

Trava Documentation (October 2022). https://docs.trava.finance/whitepaper/

Authors

Author	Twitter handle	Contact
Filippo Caprioglio	@philcapr	{filoxxx, unexployed, n0mad}@3six9.com
Unexployed	@unexployed_	
N0mad Capital	@n0madcapital	