# Fusion Credit

## Overview

Fusion Credit aims to create a credit score called the “FusionScore” based on multiple addresses and chains while keeping the account information private. Digital signature is used to ensure account ownership, and zero knowledge proof is used to hide the account information and ensure the credit score calculation is done correctly.

Like real world credit scores such as the FICO score, the FusionScore enables financial products to model risk based on individual user’s risk profile, and it is a basic building block of any financial system. Financial products, such as loans, insurance, leveraged investment accounts, etc., can offer personalized rates and services based on the credit score, making them super competitive to other products, and much more compelling to the end user.

For the credit score to be accurate and trustworthy, it needs to encompass all user activities, hence using multiple addresses on multiple chains. However, in the blockchain space, it is common to use multiple accounts for different purpose or activity, and the user may not want to make public the link between all these accounts. Fusion Credit leverages zero knowledge proof to hide all the account information, while ensuring the ownership of these accounts, as well as correct calculation process is followed to generate FusionScore off chain. Not exposing the underlying account information is the main differentiator compared to other similar products in the space.

Another unique feature of FusionScore is that the exact process to create the score is made public (built into the zero knowledge circuit). This allows the community to contribute and come up with better methodology for a more effective score. As more DeFi products comes to market, and analytics abilities improve, new FusionScore version can be created to keep up with the latest trend. Being able to upgrade the zero knowledge proof circuit is a feature built into the Fusion Credit system. The transparency will also encourage more products to use FusionScore, integrate with Fusion Credit System, and eventually create a healthy ecosystem. Any curious individuals or organization can also verify the score. In the future, a DAO can be created to govern this process of updating methodology of the score.

The high level FusionScore is rule based and can be made up with the following logical components. Machine learning can be used to create individual component scores.

- Longevity – Amount of time since the account was created
- Activity – Transactions volume, frequency, type, etc.
- Equity – Assets and properties owned, such as account balance, tokens, NFT’s
- Diversity – Interactions with different types of service
- Specialty – Depth of experience in a particular type of service
- Propriety – Having good behavior and not associated with criminals
- Ubiquity – Using multiple accounts and L1/L2 networks, or even off chain data

## Initial Architecture

The system contains three main components:

- Frontend – User interface that will perform the following
  1. Add account by user signing a message (repeat for each account)
  2. Request raw account data from server (repeat for each account)
  3. Generate zero knowledge proof which includes score calculation
  4. Submit proof and score data to smart contract
- Backend – Public service to retrieve data for one account
  1. Verify ownership of account (ECDSA signature check)
  2. Retrieve raw chain data for the given chain / network
  3. Return data with ZK friendly signature
- Smart Contract – Update and retrieve credit score data
  1. Verify proof and add score (or update score if newer version / date)
  2. Retrieve score for given address
  3. Allow zero logic proof verifier (i.e. score logic) to be updated

Note: Current design does not expose account info outside the user's browser. Which means the user is the only person that can update the score, and he/she will need to manually kick it off due to signature verification. Additional architecture needs to be designed to allow score update without end user involvement. This can potentially be achieved by storing an encrypted version of the account list on a calc server, and have the calc server re-encrypt individual address and distribute to a farm of Backend data servers to retrieve raw data. The data server only sees one address and don't know the full picture, and the calc server aggregates the data and generates the proof, but don't see the list of addresses in the clear.

## Milestones

1. Complete and deploy all system components as a proof of concept
   - FusionScore v1 with simple Longevity, Activity, Equity support
   - Signature checks to verify account ownership
   - On chain FusionScore with ZK proof
2. Meaningful score that other services can leverage
   - FusionScore v2 with Longevity, Activity, Equity, Diversity, and Specialty
   - Link score with global id system
   - Make score available on multiple chains
   - Potentially forming a DAO for governance
3. Fusion Credit system improvement
   - FusionScore v3, add Propriety (machine learning) and off chain activity
   - Allow non others to request score update
   - Improve 3rd party integration with better API

## FusionScore V1 and ZK Circuit Design

The following process is used to calculate FusionScore v1 score which has a value between 1 and 1000. We use a value of 0 to indicate non existing account.

*Score components:*
Due to complexity in utilizing machine learning models in ZK circuits, a simple system will be used for calculating the FusionScore:

- Longevity – Number of days since account was created divide by 2, up to 300
- Activity – Number of transactions in the last year, up to 300
- Equity – Account balance divide by 512, cap at max of 300
- Ubiquity – A method to combine multiple accounts to achieve better score (up to 1000)

A linear scale is used here for this initial version. Ideally, a weighed scheme should be used, either with the log function or based on the overall account population distribution. This can be implemented in a future version of FusionScore.

*Individual account score:*
The Longevity, Activity, and Equity scores summed together to create an account score between 0 and 900. Individual account scores maxed out at 900 so that it can be improved upon with multiple accounts to reach an overall score of up to 1000.

*Combining account scores:*
To combine the scores, a process that has the following properties is needed:

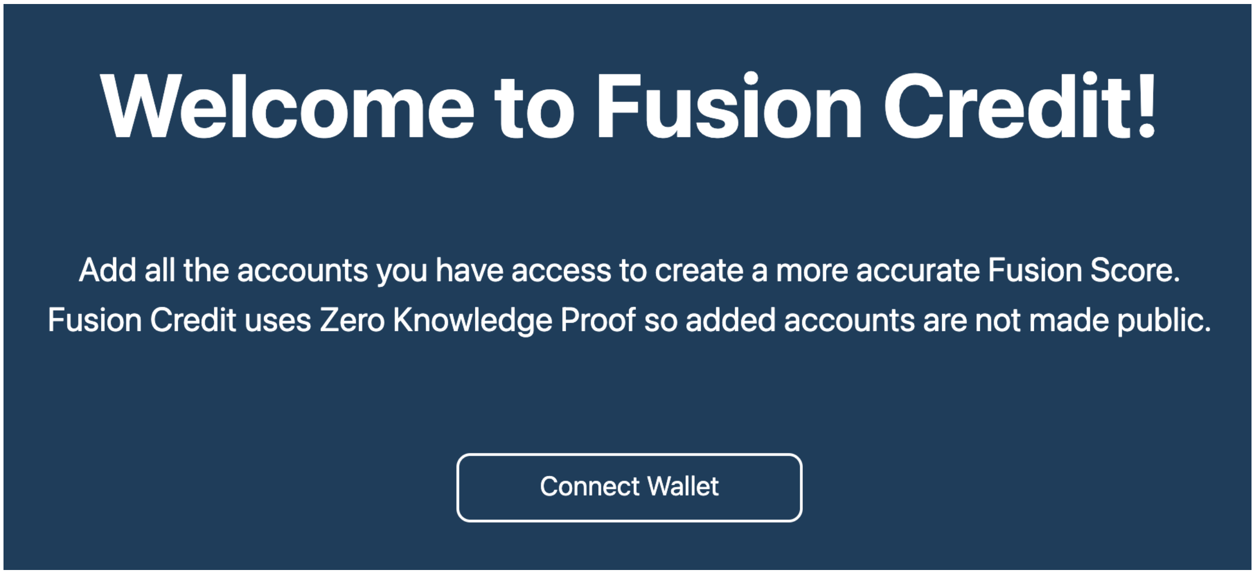
- Combining multiple scores in the range of 0 to 1000 yields a result in the same range
- The result should be larger than or equal to the maximum score being combined

For FusionScore v1, the score combining process is designed as follows:

- Scale the inputs between 1 and 2 in reverse, i.e. $(1000 - x) / 1000 + 1$
- Multiple the scaled inputs together
- Scale the output between 1 and 2, i.e. $(y - 1) / (2 ^ n - 1) + 1$ where n is the number of inputs. This result should be smaller or equal to any of the inputs
- Scale the above back to credit score range (reverse of first step), i.e. $1000 - (z - 1) * 1000$
- Note: in practice the previous two steps can be combined, and the operations need to be converted to use integer math (i.e. fixed points)
- Scaling to the range [1, 2] allow final score to converge slower to 1000. For example, combining two 900 score gets 990 using [0, 1] and only 930 using [1, 2]. To reach a 990 score, 6 accounts with 900 score is required.

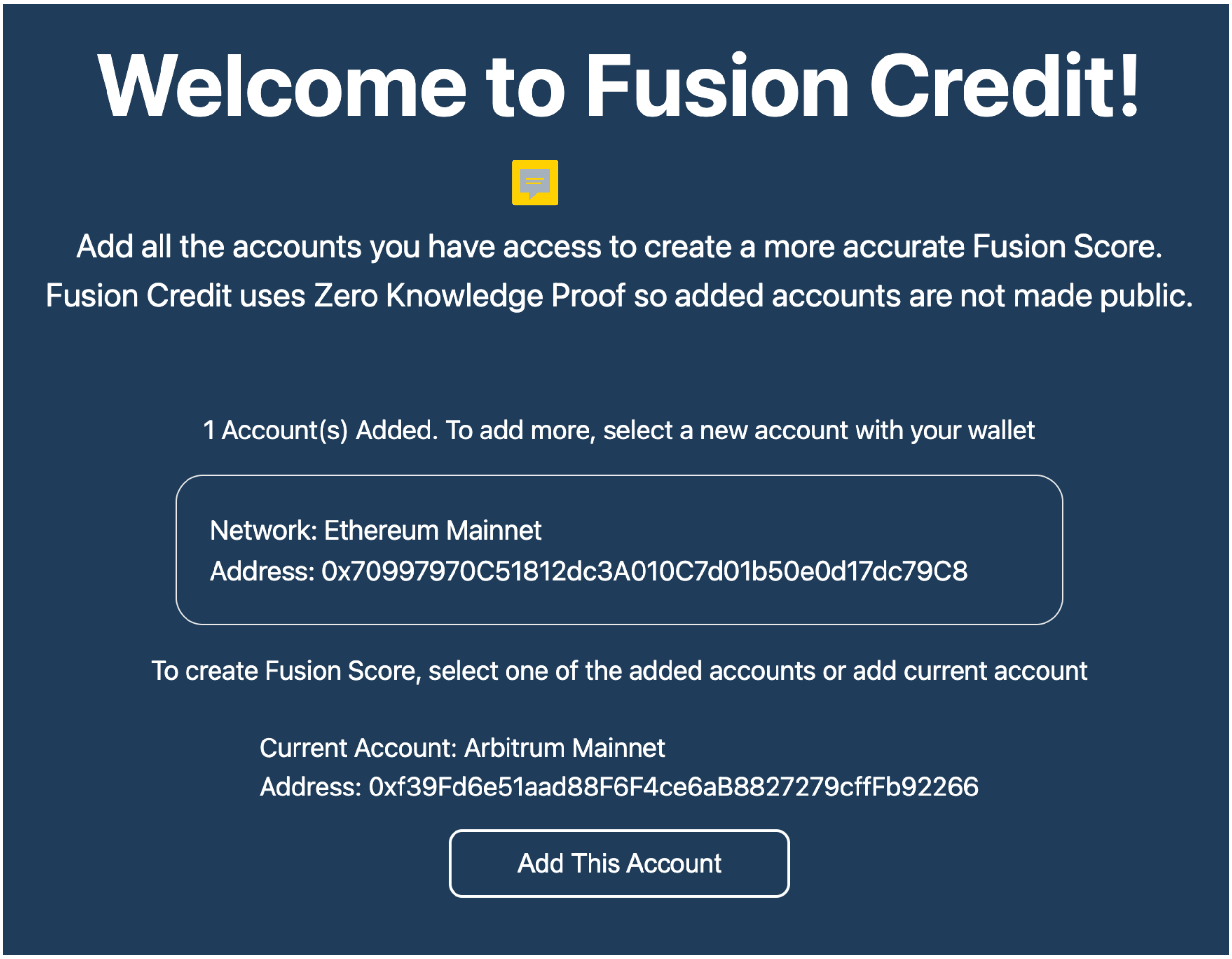
*Final Check:*
To use a score of 0 to indicate no credit score/non existing account, we force the range of valid scores to be at least 1. So if the result of the above calculation is 0, we make it 1. This is only precautionary since the original Longevity and Activity scores will not be both 0.

## User Interface



Welcome to Fusion Credit!

Add all the accounts you have access to create a more accurate Fusion Score.
Fusion Credit uses Zero Knowledge Proof so added accounts are not made public.



Welcome to Fusion Credit!

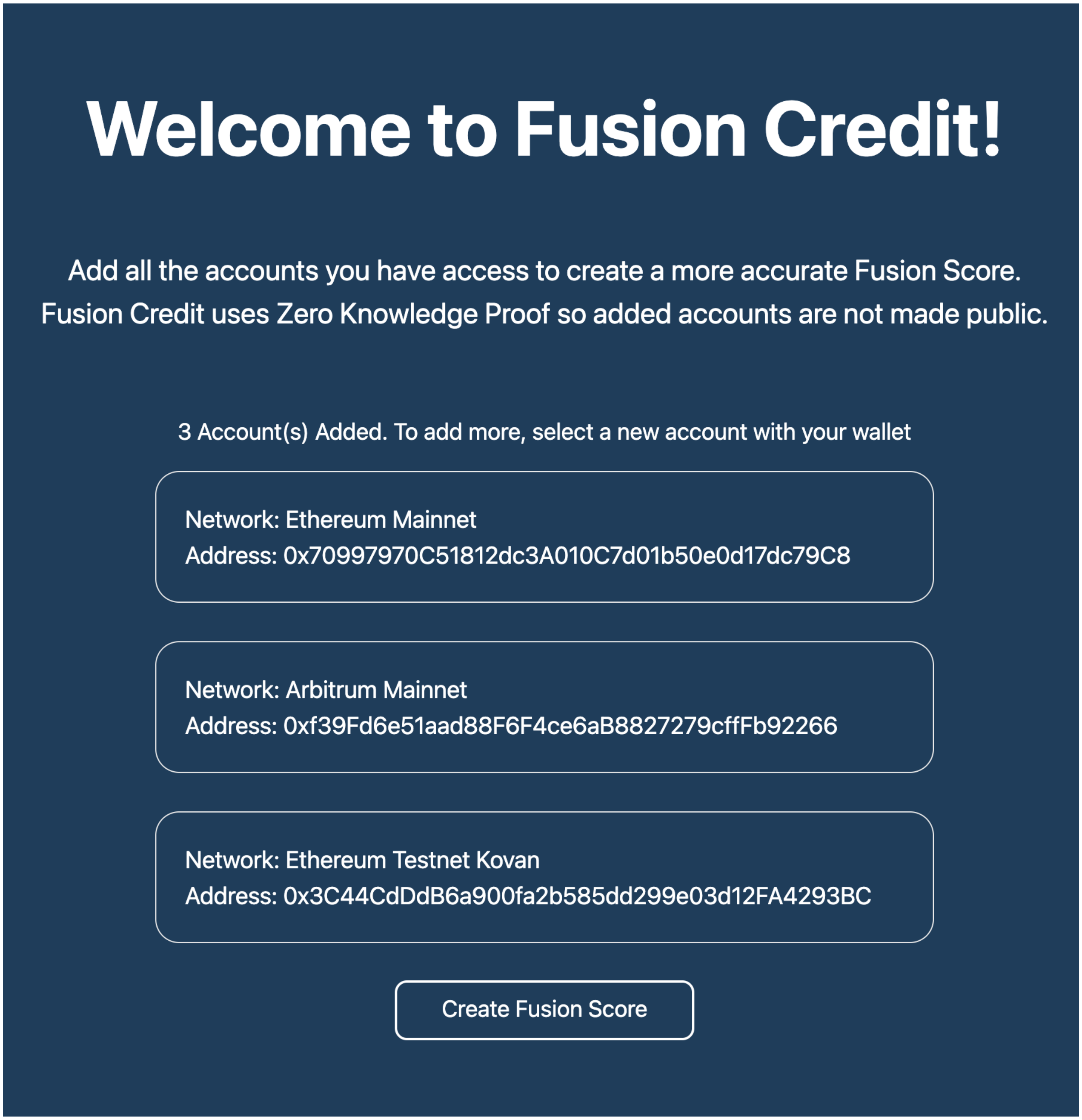
Add all the accounts you have access to create a more accurate Fusion Score.
Fusion Credit uses Zero Knowledge Proof so added accounts are not made public.

1 Account(s) Added. To add more, select a new account with your wallet

Network: Ethereum Mainnet
Address: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8

To create Fusion Score, select one of the added accounts or add current account

Current Account: Arbitrum Mainnet
Address: 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266



# Welcome to Fusion Credit!

Add all the accounts you have access to create a more accurate Fusion Score.
Fusion Credit uses Zero Knowledge Proof so added accounts are not made public.

3 Account(s) Added. To add more, select a new account with your wallet

Network: Ethereum Mainnet
Address: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8

Network: Arbitrum Mainnet
Address: 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266

Network: Ethereum Testnet Kovan
Address: 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC

## Similar Application 1: CreDA

https://creda.app

CreDA (Credit Data Alliance) is a decentralized credit rating system. The project started about a year ago. It creates a credit score between 0 and 1000 based on activities in multiple chains. Oracles are deployed to each chain to collect data from that chain. The documentation mentioned User Asset, Transaction Activity, On Chain Behavior, and Loan Participation is used to create the score with machine learning, but exact methodology to create the score is not disclosed and done off chain. The documentation mentioned that DID (Decentralized Identity, a W3C standard) is used to tie multiple accounts together, and the credit score created is linked to the DID. On top of the credit score, they have additional structures such as an NFT (does not contain the score, but indicate different levels based on the tier such as top 1% of all scores) and a Network that allow people to interact, such as serving as guarantors for others to earn a fee and improve credit score.

The project is released in Arbitrum main net with Oracles to collect data and calculate scores for BTC, ETH, BSC HECO, etc. It does not seem to integrate with any existing DID system yet (such as the Elastos DID), and looking at the code indicate the DID is generated by hashing the ETH address. The smart contract does have code to link multiple account addresses, and all the associated addresses are public on the contract. How multiple addresses are supported is not clear to me. Documentation indicates it should come from DID, but there is no code for that.

Compared to Fusion Credit, CreDA is a more mature project. Using DID to tie multiple addresses under the same identity sounds great in theory, although in practice I think there will be user experience and interoperability challenges. It also exposes all linked addresses, which Fusion Credit tries to solve. I am also guessing the score creation methodology is more sophisticated for CreDA right now (no way to compare since what CreDA uses is not public). With the transparency and upgradability of FusionScore, I believe it will become superior in the long run.

### Similar Application 2: Roci

https://roci.fi

Roci.fi is a DeFI product that support under collateralized lending. Unlike other lending platforms that require over 100% collateralization, Roci creates a credit score between 0 and 10 (lower is better) that allow trustworthy people borrow with less collateral, some even with no collateral. To create the credit score, user connects the wallet (Metamask or Ledger Hardware Wallet), and add accounts by signing a message. Once all accounts are added, they are sent to the backend which calculates the credit score (off chain) and mint an NFT that contains the score and all the account addresses. This NFT can not be transferred, but can be re-minted to update the score. Although it should be technically possible to use the score elsewhere, it seems the score is mainly catering to Roci's own deposit and lending products. For people with better credit, they offer higher interest rates for deposits, and lower collateral requirements for borrowing.

The project is currently released to Kovan test net, and I was able to mint an NFT with 3 accounts without issue. The UI looks and works reasonably well, but adding accounts from different networks is not currently supported.

Compared to Fusion Credit, Roci shares similar UI concepts of linking and authenticating accounts. But that's where the similarity ends. By having all constituent addresses public, Roci is able to ensure each address can only be used once. Compromised addresses can easily be checked, even after the score is generated. And updating the score can be done without requiring the user to enter all accounts again. While Fusion Credit hides the account accresses, these are some of the costs to pay. Roci has not published the score calculation logic, so the point above about methodology transparency with CreDA also applies here. And lastly, Fusion Credit aims to create a general-purpose credit score for crypto. Roci's coarse score (only 10 different levels), and less intuitive scaling (lower score being better) makes it harder to use by products outside of its own ecosystem.