Ormi – a decentralized, self-sovereign credit system

[Draft] October, 2021

Victor Fei, info@ormi.fi

1. Abstract

Ormi is a decentralized, universal, privacy-preserving, and self-sovereign credit system for decentralized finance. Borrowers on Ormi will be able to take out crypto loans with low collateralization based on the borrower's on-chain credit history. Ormi's identity and credit profile system is based on W3C's decentralized identifier (DID) and verifiable credential (VC) standards. Every transaction of a user with Ormi results in a verifiable credential issued and chained to the previous credential cryptographically, forming an immutable credit history and stored on IPFS, enabling Ormi to not require real-world identities or legal contracts to manage default risks. An Ormi DID with good credit history enjoys privileges in the system (lower collateralization requirement), while a suboptimal credit history requires higher collateralization requirement. Lenders and lending pools can opt in for credit default swap contracts as insurance policies for borrower default. In the event of high default rate, Ormi governance's tokens can also be minted to be auctioned on exchanges to recapitalize the lending pool, as a way to restructure debt and penalizes bad governance. Ormi employs dynamic interest rate to incentives liquidity and reduces bank run scenarios. Furthermore, Ormi's monetary policy is governed by a Decentralized Autonomous Organization (DAO), consisting of Ormi governance token holders, whose monetary policies have direct impact on the default risk and liquidity ratio of Ormi's lending pools.

2. Introduction

Credit is the granting of buying power in exchange for a promise to pay it back, which is debt. What the borrower receives in present is credit and promises to pay in the future to lender is termed debt. Credit and debt are essentially the same entity with different names.

In the traditional financial system, most consumer loans (e.g. mortgage, credit card) are in the forms of credit, little or no collateralization is required. The qualification for a loan is determined by the borrower's ability to payback, often a function of the borrower's monthly income and outstanding debts. To secure a loan using assets (e.g. real estate) as a collateral, borrowers are often subject up to 10% interest rate (hard money loan). Mainstream banks often do not offer such asset-based loans to the average consumers. In summary, in traditional finance, asset-based loans typically have higher interest rates and are less accessible. Credit based/non-collateralized loans are the norm for the average borrowers.

On the contrary, in decentralized finance (DeFi), popular lending protocols such as MakerDAO, Aave and Compound require overcollateralization (often up to 150%) for a user to borrow a different type of assets or tokens. To date, there is no widely adopted solution for undercollateralized loans in DeFi. Overcollateralization is not credit and overcollateralization is not capital efficient. Credit is a time machine that brings the value from the future into the present, in exchange for a promise for payback in

the future and often spread out over a time frame. Credit is a better utilization of capital at the present, and it does not require overcollateralization. In short, DeFi at the present state lacks undercollateralized lending and a credit system in general.

Ormi fills this protocol and infrastructure gap in DeFi and blockchain by creating a decentralized credit system, where users will be able to borrow crypto assets without the need to overcollateralize, and without relying on real-world identity or legal contracts for managing default risk.

Every lending system consists of two components:

1. Mechanism for securing the loan.
2. Mechanism for maintaining liquidity.

Popular lending protocols such as Aave and Compound secure the loan via overcollateralization and incentivizes liquidity via dynamic interest rate. Ormi predominately innovates in the mechanism for securing the loan (component 1) via reputation and partial collateralization rather than over collateralization. For incentivizing liquidity (component 2), Ormi utilizes the same interest rate mechanism as Aave, as historical data has shown the robustness of such model against bank runs.

For undercollateralized lending systems such as Ormi, there are three major challenges that may cause the system to collapse:

1. Sybil attack, numerous fake borrowers taking out loans without any intention to repay. Sybils need to be eliminated.
2. Borrowers default, legitimate borrowers unable to pay back the loan. Debt needs to be restructured and borrowers will face penalization.
3. Liquidity risk, bank run scenario, when lenders want to claim deposits but insufficient liquidity in the lending pool.

The following are the rest of the paper which will in details explain how Ormi handles the above three challenges to ensure Ormi lending system maintains healthy lending practices and liquidity ratios:

Section 3: Good credit and bad credit. The goal of any credit system is to ensure more good credit is created.

Section 4: Ormi decentralized identity and credit system. How to facilitate good credit creation and eliminate Sybil attack.

Section 5: Ormi default risk reduction system. How to handle borrower default and debt restructuring.

Section 6: Ormi lending pool and interest rate strategy. How to reduce liquidity risk and prevent bank run.

3. Good credit and Bad credit

There is good credit and bad credit.

Good credit has three characteristics:

1. Borrower will be able to pay back principal + interest.
2. Borrower's overall debt burden improves.

3. Creates more intrinsic value and economic productivity.

Bad credit also has three characteristics:

1. Borrower will have difficulty to pay back principal + interest.
2. Borrower's overall debt burden worsens.
3. Creates little or no intrinsic value and economic productivity.

The failure mode of a credit system is default, i.e. borrowers do not pay back the borrowed principal. Every sustainable credit system will have to be able to handle borrower defaults. When good credit is abundant in the system the risk of default is low, the system is sustainable. When bad credit is prevalent, individual's default risk is high, and the entire credit system can collapse.

For most sovereign states and central banks, when good credit abounds little or no intervention is needed. And it is no easy feat to facilitate that most created credit would fall under the "good credit" camp. What central banks' monetary policies are mainly concerned about is when bad credit is prevalent since bad credit and defaults can catastrophically destroy the entire economy. The tools that central banks and governments have to mitigate the risk of bad credits are: lowering interest rates to stimulate economic growth, restructuring debt burden, redistribution of wealth (raises taxes), and printing money. Note that credit systems that exist in fiat monetary system is entirely centralized. i.e. central banks' policies determine dictates creation of credit and mitigates default risks. Managing credit creation in a decentralized, open system is no easier feat than that of the central banks and sovereign states.

In summary, the cardinal principal for a credit system whether centralized or decentralized is to facilitate good credit creation. Defaulted debts can also be restructured to mitigate the impact on system and lenders.

4. Decentralized Identity and Credit Protocols

How to facilitate good credit creation and eliminate Sybil attack.

Ormi's utilize its own decentralized identifier (DID) and verifiable credentials (VC) protocols to establish identities and credit profiles for all parties that interact with Ormi. Ormi leveraging network effects of DID & VC to encourage non-fraudulent behavior and timely loan repayment. Late payment/default results in negative VC record which penalizes borrower's credit worthiness. For negative VC credit records to disincentive user from not paying back, they must be widely adopted and achieve network effects. Hence the single success indicator of Ormi's mission hinges on the adoption of Ormi DID & VC.

a. Ormi Decentralized Identifier (DID) Protocol

Ormi DID protocol utilizes blockchain as a chronological oracle to record the state and lifetime of an identifier. The user's private key controls the entire identifier. Ormi DID protocol is essentially a decentralized public key infrastructure (DPKI).

All parties that on board with Ormi protocol will be issued with a DID that uniquely identifies the party, with which verifiable credentials will be tied to the DID which forms the foundation of Ormi's identity system. Ormi DID protocol is based on the W3C Decentralized Identifier Sidetree protocol and

Microsoft's ION protocol[1]. It is a Ethereum layer 2 solution to identity, using the blockchain as an immutable chronological linear oracle to anchor the conflict-free delta updates (create, recover, update, deactivate) of an identifier.[2] The verbose delta updates is stored in Content-Addressable Storage (IPFS) and linked to the Ethereum blockchain via an anchoring string. The protocol allows users to create globally unique, transferable, and user-controlled identifiers and manage their associated PKI metadata, without need for trusted third-party. Each Ormi DID is resolved to a DID document which is in JSON containing PKI metadata such as public key references and service endpoints. The DID resolution are carried out by Ormi Identity Resolution (OIR) node instances, who perform write operations to anchor DID updates unto Ethereum blockchain and read operations to sequentially piece together DID updates to form the current DID Document state. This ability to replay these precise sequences of DID PKI state change events, and process those events using a common set of deterministic rules allow OIR nodes to achieve a consistent view of DIDs and their DID Document states, without requiring any additional consensus mechanism or tokens. Ormi Identity Resolution node will be open sourced and can be deployed by anyone. Ormi development team will initially maintain several OIR nodes to ensure Ormi DID resolution uptime. To ensure distribution and decentralization of OIR nodes in the future, Ormi will consider incentivizing deployers of OIR nodes via Ormi tokens.

To create an Ormi DID, a user's pre-existing Ethereum address can be used as an Ormi DID. The user can later also transfer or tie a different Ethereum address to Ormi DID. In fact, since the Ethereum blockchain is only used as a chronological oracle for anchoring identifier state updates, the user can in fact associate other blockchain addresses with Ormi DID. In addition, Ormi DID conforms with the W3C DID standards, which ensures compatibility with other DID providers and services, including governmental agencies and corporations[3].

TODO: Architecture diagram of Ormi DID protocol.

b. Ormi Verifiable Credential (VC) & Credit Profile

VC are credentials cryptographically signed by an issuer DID issued to a holder DID, who can then present the VC to a verifier DID to prove a claim the issuer made about the holder. VCs reside off-chain in Content-Addressable-Storage (IPFS). Each Ormi VC is essentially a credit history attestation associated with a DID.

Ormi utilizes the verifiable credential following W3C standard[i] to represent a DID's credit profile. When a issuer issues a verifiable credential to a holder. The issuer signs the credential with the private key of the issuer's DID to the holder. Upon request for presentation by a verifier, the holder signs the VC with his own private key, and presents the VC to the verifier. The verifier will be able to verify the authenticity and identity of the issuer and presenter by looking for their public key on Ormi Identity system. Ormi DID system acts as a decentralized PKI.

---

[1] Microsoft ION uses Bitcoin to anchor the DIDs. https://identity.foundation/ion/

[2] https://www.w3.org/TR/did-core/
https://identity.foundation/sidetree/spec/

[3] The decentralized identity foundation (DIF) is a consortium of industry partners for developing DID standards and solutions. For a list DIF corporations and governmental agencies that are currently seeking decentralized identity solutions, see https://identity.foundation/

Originally, VCs are intended to reside offline, in individual's crypto-wallets. The individual can then selectively disclose/present these VCs to a requestor. Akin to the physical world, where a driver's license resides in a physical wallet and the holder presents the driver's license to the requester. VCs were also originally designed to be single use case credential (e.g. driver's license) rather than credentials that are linked together (e.g. credit history). They were also intended not to be stored on centralized servers or distributed CAS (e.g. IPFS). However, due to VC wallet applications are not widely adopted, Ormi stores the temper-proof cryptographically linked together VCs (i.e. credit history) on IPFS for easy access.

Ormi credit history is privacy preserving and can only be read by the holder and requestor (upon holder approval). Each credit activity VC issued by Ormi lending protocol is first signed with Ormi's private key, then encrypted with the holder's public key before writing to IPFS. So that only the holder can read the issued credentials via decrypting with his private key (figure 1).

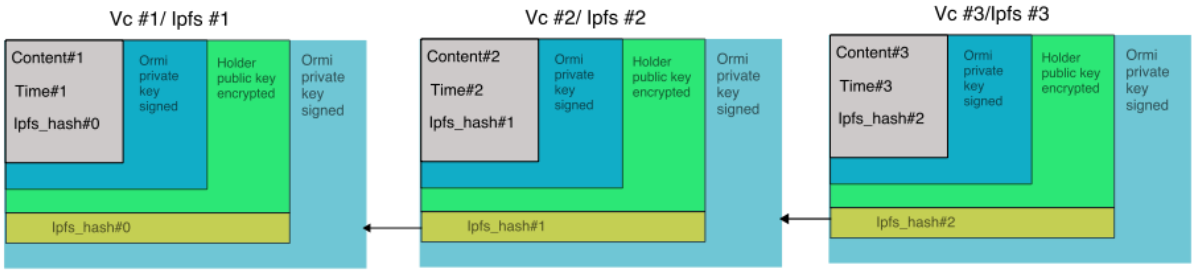

Figure 1

When the holder makes a presentation to lending protocol (e.g. Ormi), attesting the his own credit worthiness, the holder first retrieves and decrypts the credit history from IPFS onto his own local storage as outlined before (figure 2).

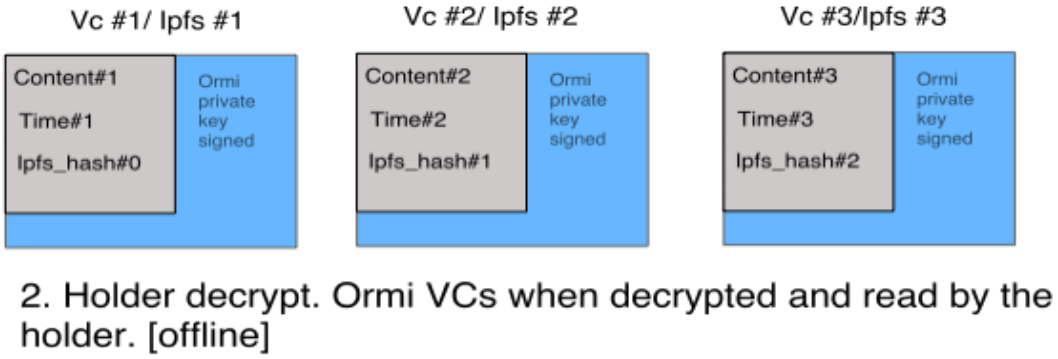

Figure 2

Then the holder encrypts the credit history with the verifier's (i.e. Ormi lending contract's) public key and delivers over the network the encrypted VC to the verifier. The verifier then uses his own private key to decrypt the credit history and utilizes Ormi DID system (DPKI) to verify the authenticity of the VCs (figure 3).

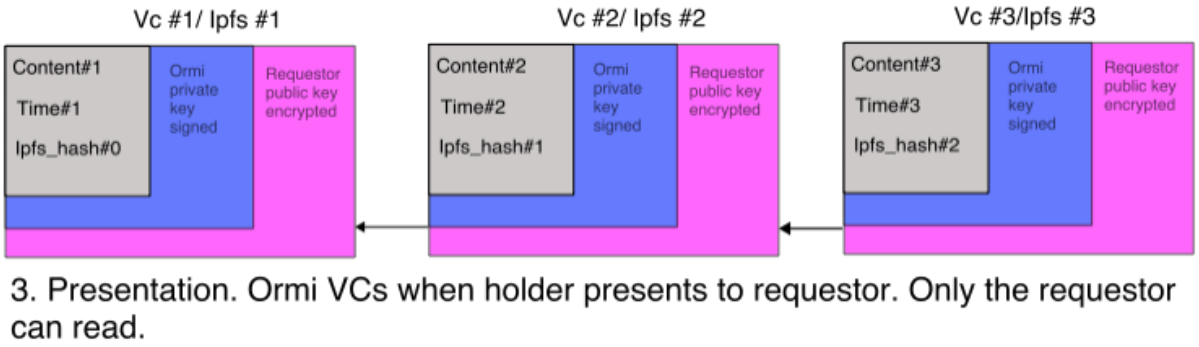

Figure 3

In summary, Ormi credit history is formed by cryptographically chaining individual VCs and commit to IPFS. These chained VCs (credit history) are tamper-proof, changing each VC (credit activity) resulting in the whole VC chain (credit history) being invalidated. Once issued, the access of an individual's credit history is only limited to holder, who then decrypts and presents to the verifier/requestor, thus preserving credit history's privacy.

c. DID onboarding & Sybil control

To create an Ormi DID, user will be able to 1. directly onboard an existing Ethereum address 2. create a brand new Ormi DID and then associate different Ethereum address owned by the user. An Ormi DID is typically associated with Ethereum address(es) as a form of Sybil control to ultimately reduce borrower default risk. SybilRank type of algorithm[4] is run on each Ethereum address to attest the trustworthiness of each address.

If the Ormi DID does not have any associated Ethereum address or its trustworthiness cannot be determined at the time of onboarding, the Ormi DID will not be able to leverage undercollateralized position. Only by extensively interacting with Ormi lending protocol, i.e. building up credit history, can an untrusted Ormi DID utilize undercollateralized position.

5. Default risk reduction and debt restructuring.

How to reduce default risk, manage borrower defaults, and restructure debt

Protocols such as Aave and Compound utilizes overcollateralization to secure the loan and eliminate default risk. When a loan is not secured by 100% collateralization, default risk will always remain. Ormi only aims to reduce such default risk, but never eliminates it. When borrowers default, borrowers gets penalized and debt gets restructured.

Default risk reduction

It is virtually impossible to eliminate all default risks for undercollateralized positions. Even in traditional financial systems, creditors prefer to reduce the chances of borrower default (e.g. credit history check)

[4] BrightID/BrightID-AntiSybil: Sybil detection package for BrightID (github.com)

in the first place, rather than debt collection. In the case of sovereign states default, there are even fewer actions can be taken to reclaim the debt. The only penalties that defaulted sovereign state suffer is more difficulty to borrow in the future. Seldomly do creditor countries use military to take over the indebted countries due to defaults. In the actual event of default, the defaulted debt is compensated often via debt restructuring.

Similarly, Ormi does not guarantee zero default risk for undercollateralized positions. Ormi reduces the overall default risks by encouraging issuance of "good credit" and non-fraudulent behaviors via the following implementations:

1. Leveraging network effects and reputation of Ormi DID & VC
2. Partial collateralization and slashing penalty

a. Ormi DID & VC reputation

Leveraging network effects of the adoption of Ormi DID & VC to encourage non-fraudulent behavior and timely loan repayment. Late payment/default results in negative VC record and credit history which penalizes borrower's credit worthiness. For negative VC credit records to discourage user from not paying back, they must be widely adopted and achieve network effects. Hence the single success indicator of Ormi's mission hinges on the adoption of Ormi DID & VC. Previously mentioned, onboarding Ormi DID & VC requirements for Sybil control also contributes to preventing fraudulent behavior.

b. Slashing penalties

Ormi initially does not aim to achieve zero-collateralization but rather low collateralization ratio (< 100%) dynamically based on default risk factor. Borrowers are required to deposit collateral as a form of Sybil control mechanism and encourages good behavior. Slashing entails all collateral will be liquidated upon borrower default. In the later iteration of Ormi protocol, zero-collateralization loans will be explored.

c. Variable collateralization ratio and VC reputation

The collateralization ratio of a DID is based on it's past history interacting with Ormi protocol. A user/DID with favorable past history (repaying loan on time, no liquidation) enjoys the privilege of lower required collateralization ratio, while a user with unfavorable or non-existent past history will be required with higher collateralization amount. Each loan activity (interest payment, liquidation, default, etc), a VC is generated to represent the user/DID's credit history as described in Section 4. All users start with 100% collateralization ratio and after certain period and number of favorable loan activities (e.g. closing a loan), a user's collateralization ratio will be lowered linearly to 90%, then 80%, 70%, etc. Upon unfavorable loan activity (e.g. default) the collateralization ratio of a DID will increase exponentially.

For loans with higher collateral ratio (say >50%), no time limitation is imposed on the loan as long as the minimum collateralization is met. For loans with lower collateral ratio, a time limit will be imposed. For such positions, failure to close out the loan by the end of the loan term will result in the liquidation of collateral and negative VC issued. The exact collateral threshold that results in a time-limited loan needs to be found out via experimentation.

Debt restructuring

d. Ormi treasury

An Ormi treasury is setup to recapitalize the lending pools from the loss of small scale, individual defaults. The Ormi treasury funds result from a percentage of repaid borrower interest.

e. Minting & auctioning governance token

Since governance token holders have the responsibilities of ensuring sound monetary policies for the protocol to reduce default risk, should widespread defaults occur, governance token holder should be penalized and pay for debt restructuring. This is done via minting more governance tokens to sold on secondary markets to raise funds to recapitalize the liquidity pools. Due to the increase of supply of Ormi governance token, its value will decrease. It is in governance token holder's interest to ensure sound monetary policies and only good credits are created. This is equivalent to "tax" the governance token holders to restructure defaulted loan.

[TODO] Borrower default risk parameter calculation

[TODO] System default risk parameter calculation

[TODO] Interest rate as a function of default risk and collateralization ratio

TODO: What interest to charge so it covers default as a function of individual default risk and collateralization ratio.

6. Liquidity, lending pool, and interest rate strategy

How to reduce liquidity risk and prevent bank run

Ormi follows the precedents set by existing lending protocol such as Aave and Compound and uses a lending pool model with variable interest rate to incentivizes liquidity. Ormi lending pool supports multiple types of collaterals.

a. Variable Interest Rate Strategy

Ormi's variable interest rate strategy follows a kinked rates model as seen in Aave and Compound protocol. The interest rate rises sharply at some defined threshold as a function of utilization rate to incentivize more liquidity supply from lenders, as an effort to decrease utilization rate and increase reserve ratio.

$$R_v = \begin{cases} R_{v0} + \dfrac{U}{U_{optimal}} R_{slope1}, & U \leq U_{optimal} \\ R_{v0} + R_{slope1} + \dfrac{U - U_{optimal}}{1 - U_{optimal}} R_{slope2}, & U \geq U_{optimal} \end{cases}$$

Note that borrower default will also contribute to the amount of available capital, which will in turn decrease reserve ratio and increases utilization rate.

b. Stable Interest Rate Strategy

Ormi also supports stable interest rate strategy and follows that of Aave, where user pays for a premium to lock in a stable rate adjustment until utilization rate is above $U_{optimal}$ at which point stable rate rebalances occurs.

c. Market volatility

1. Bear market or strong volatility, collateralization ratio will increase. Somewhat parallel to traditional finance, when the economy is booming, asset prices are increasing, credit is cheap and abundant. When economy is contracting, asset prices are falling, credit can be expensive and risky, hence higher amount of collateralization is required.
2. In case of black swan event, or bank runs that cannot be controlled, emergency protocol will be activated to free all funds and withdraw

7. Conclusion

The Ormi system relies on lending pool model and variable interest rate to control liquidity supply to ensure high liquidity. Loans are represented by oTokens, derivative tokens which accrues the interests for holders. The key innovation of Ormi is loans are backed by borrowers' on-chain credit history verifiable credentials and partial collateralization, rather than over-collateralized crypto assets. In the event of borrower defaults, debts are restructured via credit default swap and minting Ormi governance token to be traded on exchanges to cover defaulted debt in pools.

In summary, Ormi improves decentralized finance's current offering by the following two key innovations:

- Ormi decentralized identifier and verifiable credentials to establish identity and credit history to allow for loans to be backed partially by reputation.
- Debt restructuring to recapitalize the loss of liquidity due to defaulted loans via treasury, insurance contracts, and minting and selling governance tokens.

Following the launch of the mainnet, Ormi will uphold its commitment to decentralization through fine tuning of various parameters to allow more undercollateralization while maintaining safety and introduce additional features to further evolve Ormi system and the DeFi ecosystem.

Governance will be on-chain with rights represented by:

- Ormi token at protocol level for update of the smart contracts and monetary policies.
- oTokens at pool level for pool specific parameters.