Introducing Self-Sovereign Identity and Identity as Collateral in Decentralized Finance

Harmen Kroon , Martijn de Vos , Johan Pouwelse
TU Delft

Abstract

Decentralized Finance (DeFi) is build on smart-contract supporting blockchains, with Ethereum being the largest ecosystem. A collection of smart-contracts aims to serve as decentralized implementations of financial systems. The philosophy of DeFi dictates automation and desintermediation through exploiting nascent distributed ledger technology and cryptoanarchist ideologies. Interest in DeFi has risen in the past year, with total value locked in Ethereum based decentralized applications having multiplied fiftyfold. Lending is one of the main building blocks of finance and DeFi protocols try to provide that service. Lending services offer liquidity in exchange for counterparty guarantee. Due to the pseudonymous nature of DeFi that guarantee is limited to collateral, which is expressed in overcollateralization as a result of cryptomarket volatility. A persistent, untamperable and uniquely identifiable credit history opens the door for counterparty guarantee without liquid collateral. Uncollateralized lending lowers a barrier of entry for mainstream adoption of Decentralized Finance. This paper proposes a novel solution to cryptographically secured loans in a decentralized system by presenting a credit history linked to a persistent self-sovereign identity.

1 Introduction

Trust in the traditional banking and finance world has fallen after the 2008 financial crisis and more recently the COVID-19 financial fall. Nakamoto [1] proposed a peer-to-peer electronic cash system based on cryptographic proofs and chained transactions, which propelled the world into cryptocurrency finance. Public blockchains have evolved from the original bitcoin paper and enabled the building of decentralized applications on distributed ecosystems and thus the term Decentralized Finance (DeFi) is coined. The basis that facilitates the DeFi ideals of an open and global financial system are four properties: *non-custodial*, *permissionles*, *openly auditable* and *composable* [2]. These properties have been applied to one of the building blocks of finance in lending and borrowing, through Loanable Fund Markets [3]. These markets offer two distinct types of loans. Flash loans are secured as a single atomic transaction which can be reverted in case the loan defaults [4]. Collateralized loans span longer terms and are secured by fully collateralizing the loan with crypto assets.

The DeFi market picked up momentum in 2020 and as of June 2021 the DeFi market's size, measured in Total Value Locked, was estimated to be approximately \$ 50 billion[1] and Monthly Trading Volume surpassing the trillion dollar mark in February 2021 [5]. The largest contributors in this space are financial trading institutions that see potential in the high yield promising markets, but DeFi has begun to cross the threshold to mainstream consumer fintech apps [6]. Participation in alternative finance through fintech is growing under consumers, indicating a potential market in DeFi lending that is currently gated by a barrier of entry [7].

Considering that lending requires some form of guarantee to counterparty risk, traditional finance has applied risk assessment and post loan management to evaluate borrowers on their creditworthiness and mitigate losses. That guarantee has been secured in DeFi lending through the use of collateral, that is liquidized in case of default or fluctuations of asset value. This collateral requirement introduces opportunity cost and reduces the potential use cases of DeFi lending to margin trading and yield farming [8], thus hindering adoption of smaller speculators and non-crypto holders.

Harwick & Caton [9] offer an institutional and technical perspective that suggests offering an identity link to transparently manage counterparty risk is a solution towards uncollateralized lending. As traditional and alternative banking are increasingly regulated on digital identity privacy and security [10] as well as Know Your Customer and Anti-Money Laundering compliance [11], so is the push for adoption of compliant privacy preserving identity solutions [13]. A modern digital identity solution that shares many ideological values with DeFi, is Self-Sovereign Identity (SSI) [14]. A Legally Enabled SSI opens the door to legally compliant and identity persistent digital finance by privately storing and enabling presentation of credit history. Applying SSI enables bridging the trustlessness between lenders and borrowers in the DeFi space.

[1] https://defipulse.com

Therefore, the main research question this paper aims to answer is as follows:

How can a Self-Sovereign Identity enable uncollateralized loans in decentralised lending protocols?

To understand how overcollateralization is solved in current decentralized financial ecosystem the following subquestion arises: *What counterparty guarantee is used in decentralized lending protocols instead of liquid collateral?*

In order to answer these questions the following topics will be discussed in this paper. Firstly, in section 2 the established decentralized lending protocols and risk assessment are reviewed which aims to answer the subquestion. Secondly, related work is discussed in section **??**. Thirdly, identity management in decentralized finance is discussed in section 4 Finally, an implementation is proposed based on these findings using a blockchain based SSI solution and both a credit score claim and a credit history evaluation in section 5.

2 Decentralized Lending protocols

The decentralization of finance using distributed ledger technology is largely build on smart contract enabled blockchains, mainly on the Ethereum blockchain. Of the 236 DeFi projects listed on DeFiprime[2] the Ethereum ecosystem hosts 218 projects build on top of the smart contract infrastructure. Smart contracts offer a deterministic custodian for handling asset exchange based on the rules set by the contract's code. The code of contracts is publicly stored on the blockchain and open for scrutiny by the community, although security audits are the standard. Decentralized lending markets are built on smart contracts that enforce the set rules of the lending protocol, such as interest rate, collateral rate. Traditional intermediaries are therefore replaced by automation. DeFi lending is unique in that both borrowers and lenders are not required to identify themselves. Following the property of *permissionless*, everyone has access to the platform and is able to borrow money or provide funds to earn interest [12]. To ensure third party risk there are two distinct varieties of lending markets, short term loans and longer term loans.

Short term loans or flash loans are funded and repaid in an atomic blockchain transaction. If the borrower is not able to repay the loan inside of the block creation timeframe, then the transaction is entirely reverted. Flash loans therefore require no collateral at all. They are mostly used for arbitrage, (anti-)liquidation and collateral swapping [4]. Since administration of flash loans is in such a small timeframe, borrowers can only interact with the service through smart contracts. Flash loans are unique to the DeFi and the implications for finance are underresearched [4].

Longer term loans in DeFi commonly require a collateral in order to secure the loan from risk of defaulting. Lending protocols are build on the assumption of self-centered anonymous financial agents that only act in their own benefit [9]. Meaning that when it is financially favourable to default on a loan and take the loss on the collateral, an agent will take that approach. The required collateral is therefore at least as large as the loan size plus interest. In actuality collateral requirements are even higher starting at 150% of the loan size and reportedly[3] going over 300%, which is called overcollateralization. Due to volatility of cryptomarkets the value of a collateral can swing wide over the course of a loan. In the case that the value of the provided collateral falls below a protocol specific threshold a liquidation procedure ensures that capital is retrieved by selling of the collateral [4]. Another means of collateralization is through NFTs. Teller[5] sold tiered NFTs specifically for this use case and allows borrowers to post the NFT as collateral for a loan with a credit limit equivalent to the NFT tier. Efforts have been made to reduce collateral. Todd[8] describes the state of the crypto credit ecosystem and identifies the issue of overcollateralization in the lending market. The lost opportunity cost is immense as over $ 25 billion is locked in lending protocols as of May 2021. Collateral reduction mechanisms are based on building up a lending history and slowly reducing required collateral up to 100% (Balance [15], Promise [16]). The real strides are made in protocols that strive for lending with no collateral at all, similar to traditional lending. This requires a greater form of trust in the borrower, counter to that of the collateral provided trust used in secured loans.

2.1 Uncollateralized loans

Traditionally, banks secure loans through some form of trust relationship with the borrower. A guarantee for loan repayment is founded on insight into financial information and credit history along with a backstop in case of default. Where collateral acts as the backstop in secured lending, a legal identity relationship provides the backstop in unsecured lending. Trust needs to be reintroduced into the trustless decentralized finance in order to make uncollateralized lending possible. Current uncollateralized lending protocols apply an off-chain solution of identity information to establish trust.

The Aave protocol has a feature called credit delegation that allows depositors to delegate borrowing power to other users[6]. A delegator is encouraged to set up a legally binding contract with the delegatee outside of the protocol through a legal institution or through a smart contract like OpenLaw[7], which does require legal addresses of both borrower and lender depending on jurisdiction.

The latest round of DeFi protocols that aim to provide uncollateralized loans take a careful approach when it comes to approving borrowers. TrustTokens' TrueFi started out with a KYB approach and uses *"a whitelist of carefully selected funds vetted by the TrustToken team."*[8] and is evolving into

[2] DeFiprime aggregates a list of active DeFi projects - https://defiprime.com/ethereum

[3] https://smartcredit.io/why-is-the-collateral-ratio-so-high-in-defi/

[4] https://docs.aave.com/risk/asset-risk/risk-parameters

[5] teller.finance

[6] https://docs.aave.com/developers/v/1.0/developing-on-aave/the-protocol/credit-delegation

[7] https://www.openlaw.io/

[8] https://blog.trusttoken.com/introducing-truefi-the-defi-protocol-for-uncollateralized-lending-9bfd6594a48

a credit rating system in their latest version(v3). The TrueFi creditworthiness score (from 0 to 255) is based on five factors; Company Background, Repayment History, Operating & Trading History, Assets Under Management and Credit Metrics[9]. Currently this score is administered by internal analysts without much transparency.

Maple[10] is a decentralized corporate credit market that allows communities to set up their own lending pool with community driven collateralization rates. Each community is responsible for their own risk assessment. Each pool is managed by a pool delegate that stakes governance tokens as collateral for default, which has similarities to Aave's credit delegation. The protocol allows users to log in to through MetaMask, a DeFi smart wallet, as an identity provider.

C.R.E.A.M.[11] also applies a whitelisting methodology for uncollateralized protocol-to-protocol loans, under discretion of the developers. Factors that determine creditworthiness of protocols are reputation, track record, smart contract audits, insurance coverage and escrowed tokens.

Teller[17] is an algorithmic risk protocol for decentralized lending that uses distributed cloud nodes as a data router for smart contracts [18]. Teller uses data provided by whitelisted data providers and plans to use enclaves and zk-SNARKS. A credit risk algorithm uses the data to assess default risk and generate loan terms based on creditworthiness. Setting up requires a Wallet, Ethereum address, Twitter Handle and e-mail. For borrowers to take out unsecured loans using the Teller Protocol, they have to link their bank account via Plaid[12]. Undercollateralized loans are kept in escrow and only fungible at preapproved dApps[19].

Outside of the crypto-based DeFi ecosystem are organizations that apply the distributed ledger technology and decentralization to real world markets. Kiva[20] is a non profit organization that facilitates uncollateralized loans and financial services for the unbanked of Sierra Leone through an Hyperledger-based SSI[21] and peer-2-peer lending platform. The protocol specifically designed in conjunction with Sierra Leone's National Digital Identity Platform is a private, permissioned system wherein the trust anchors are approved by Kiva and the government of Sierra Leone. Borrowers store verifiable claims of loan details and repayments on their private credit ledger, allowing them the control in who they share their credit history with.

Colendi[22] is a decentralized credit scoring protocol and micro-credit platform. It uses mobile phone and social media data to compute credit scores for the unbanked and establishes lines of credit through micro loans. It uses Enigma as a Secure Computation Environment and Storj as Secure Object Storage.

The common approach to onboarding borrowers in unsecured lending in DeFi is through the use of non-automated, internal risk analysis and focusing on established trading institutions. Currently only Teller provides a link to a consumer's traditional financial institutions, although in practice most loans are still collateralized with their internal collateral NFT. Looking at micro finance platforms that actually aim to reach the unbanked of certain areas, they show that building up a credit history through microloans is a valid approach for the lower spectrum of borrowers. These two different approaches illustrate the different needs for lending markets catered to either consumer lending or trading loans.

3 Related Work

In this section research papers related to the intersection of Distributed Ledger Technology and Credit are discussed. Research focusing on Decentralized Finance is scarce and mostly analyses the incredible growth of the market.

Harwick & Caton[9] lays out the incentive-incompatibility in unsecured lending in a pseudonymous environment. Due to the inability of distinguishing between honest and opportunistic defaults. They propose a possible solution using oracles that provide contingent pseudonimity. In case of a default the oracle that verified the identity of the borrower is programmed to release identity information to the lender.

Chen et al.[23] identify issues in fiancial blockchain research, such as privacy risks of storing on-chain credit information and the similarities in weaknesses of post-loan management between traditional finance and blockchain-based finance.

Dong et al.[24] proposes a blockchain based model for open banking using SSI. Their solution uses Uport as an SSI provider promising privacy and data protection during data sharing, user-controlled identity data and identity recovery.

Rakkini & Geetha[25] proposes a blockchain-enabled microfinance model using a decentralized autonomous organization. They provide borrower incentive through the use of peer groups and monthly subscription fees. This model is similar to the South-African Stokvel rotating credit-union like scheme that is based on peer-pressure and peer-support.

Wang et al.[26] proposes a Hyperledger Fabric based smart contract solution for managing loans on-chain.

Hasija et al.[27] proposes a blockchain and prospect-theory based decentralized credit model.

Sharma et al.[28] proposes a blockchain framework for managing patients' electronic health records access control and funds. They provide transparant and auditable acces via smart contracts. Identity authentication is done through zero-knowledge proofs and access is delegated using proxy re-encryption.

4 Identity management in decentralized finance

The financial transactions in decentralized finance are made possible through sending tokens from one address to another. Such an address is pseudonymous by design as there is no direct link between the address and personal identifiable information. Therefore, the address of a known agent is commonly linked to identifying information by a protocol in order to establish some form of relationship as shown in section 2.1. Digital wallets allow users to organize their addresses

[9] https://blog.trusttoken.com/truefi-v3-credit-model-new-asset-support-a7cf73a37270

[10] maple.finance

[11] https://docs.cream.finance/iron-bank/faq

[12] Plaid is a platform that connects banks and financial apps - https://plaid.com

and give consent to protocols for accessing their address and using that as an identifier. DeFi protocols are designed on principal to allow users to interact with the protocol solely by sending and receiving assets through their address and a smart contract.

4.1 Identity Management in Decentralized Finance

A sense of financial identity can be derived from the transactions, all visible and immutable on the public blockchain, in order to procure a relationship between users and protocols. Providing users of the network an interface that allows control over their assets and addresses is essential for usability and therefore digital asset management or a wallet is used. Wallets provide ownership of an address and an interface to interact with decentralized applications. Web 3.0 wallets uses an Ethereum address and offer a keypair to the user for safekeeping thus facilitating self-custody[13].Some companies have tried implementing more capable identity solutions and even tried following the SSI principles. Uport/Serto ID management is deprecated project that offered identity solution on the Ethereum blockchain [33]. They offered an open protocol that pioneered the use of decentralized identifiers and resolvers available via open-source libraries[14]. MYKEY uses smart contracts to store personal data to facilitate a consistent crosschain ID [29]. Instead of relying on an Ethereum address as an identifier they offer Key ID usernames, which are auctioned off to the highest bidder. Bloom is an SSI solution with a build in credit score [31]. The Bloom protocol is based on three systems in order to provide identity, risk assessment and credit history; BloomID, BloomScore and BloomIQ respectively [32]. The BloomID is a collection of attestations and a peer-to-peer staking network. The BloomScore offers individuals without a credit history a way to increase their score by reflecting of the scores in their social network. Since 2020 they have been working closely with the Decentralized Identity Foundation [15].

Other identity solutions in that use distributed ledger technology are sidechain solutions and permissioned blockchain projects. Sidetree is a layer 2 protocol that enables a scalable W3C Decentralized Identifier [34] anchored to any existing decentralized ledger system[35]. The Sidetree protocol is implemented in ION for the bitcoin blockchain[36]. ION is able to fit 10,000 ID operation on a single bitcoin transaction and uses ION nodes in an IPFS. Hyperledger Indy is created and managed by the Linux Foundation. The biggest user is the Sovrin Foundation for the Sovrin network identity management system [37]. Concordium is a blockchain project with an integrated identity layer based on research by the Damgård et al. [38].

4.2 Self-Sovereign Identity

A Self-Sovereign Identity system as proposed originally by Christopher Allen is based on the principle that an identity subject has control over their own identity and all related credentials. This form of control allows an identity holder to specify if and when another party is allowed to view an identity credential, contrary to how contemporary digital identity solutions consolidate data to the identity provider. In order to prove validity of identity credentials an SSI system needs a mechanism that can verify correctness. Research shows that that a flow of trust that includes three separate parties enables verifiable credentials. In this flow the central party is the identity subject that holds all credentials. The subject obtains credentials from an authority that attests credentials and the subject proposes credentials to a third party, the verifier, that wants to verify those credentials.

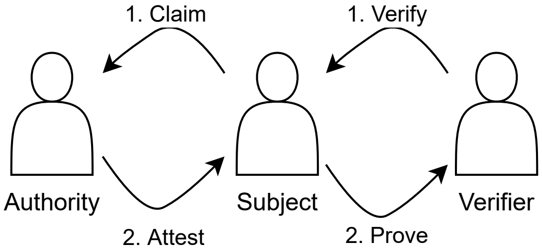

Figure 1: Credential interaction between the three parties in a self-sovereign identity system: Authority, Subject and Verifier

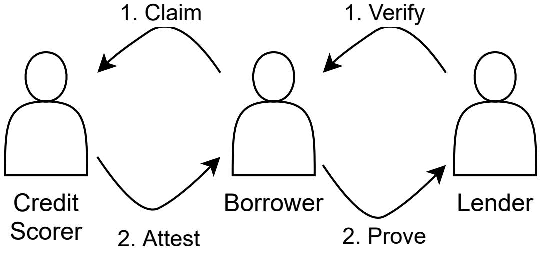

Figure 2: Credential interaction between the three parties in a loan application procedure: Credit Scorer, Borrower and Lender

Stokkink et al.[39] proposes a claim based SSI where a subject claims a credential with the authority that then decides to attest such a claim. The authority attests a claim by signing it and sending it back to the subject, who then signs the claim again resulting in two signatures. Whenever a subject provides a credential to a verifier these signatures are presented along with the identity data. A verifier is then able to verify the signature of the authority attesting the legitimacy of the credential.

The signatures used in this flow are derived from a public-private key pair from the in 1991 conceived concept called Pretty Good Privacy [40]. A signature is created using ones private key and send to an other party by encrypting it with their public key. The other party can then decrypt the message using their private key. In this asymmetric encryption scheme it is imperative that private keys are kept secure and in control of the holder of the keys. Using keys in decentralized environments requires a public key infrastructure to securely deliver public keys [41]. Building on PKI dötling and Nishimaki [42] explore a universal methodology to construct the system called Universal Proxy Re-Encryption(UPRE). PRE [43] allows a proxy to transform cipher text from one public

[13] https://defiprime.com/assets-management-tools

[14] https://github.com/uport-project/veramo

[15] https://identity.foundation/

key to another without opportunity to observe content.

Along side of the encryption of messages, the data that signifies a credential can be shared in a minimalist way by making use of zero-knowledge proofs [44]. Zero-knowledge proofs are widely used in self-sovereign identity solutions [45; 46] and are being applied to decentralized finance in the form of currency[16] or scalability[17].

Translating this flow of trust with its roles to a financial setting and specifically lending is visible in figure 2. Say, Alice wants to take out a loan with their traditional bank. The bank has knowledge of Alice in the form of their bank account history, such as income and monthly expenses, and is thus able to assess the risk of issuing a loan to Alice. Translating this flow of trust to current decentralized finance has similarities but misses one critical attribute, the verifiable identity of the borrower. As DeFi is based on distributed ledger technology, transactions are immutable and thus an account history can still be tied to one blockchain address. However, due to the mantra of DeFi this address is pseudonymous by definition; no legal identity is tied to an address.

Naturally, the problem that decentralized lending has and the problem that Self-Sovereign Identity tries to solve overlap. This forms the basis of the solution presented in section 5.

5 Our solution

SSI enabled unsecured decentralized lending systems require three main components: an SSI solution, a finance application and credential storage. The three roles of the credential trust flow, see figure 1 are equivalent to the three roles of the lending application flow, see figure 2. The borrower acts as the subject, the risk assessment protocol acts as the authority and the lending protocol acts as the verifier.

The current flaws in unsecured decentralized lending can be overcome by utilizing three components presented in our solution. A persistent identity in the form of SSI allows a user control over their financial and personal identity information without sacrificing anonymity in case of honest behaviour. The SSI must be able to securely store verified credentials of the user and offer verified presentations with the users consent. Additionally, the SSI solution must be able to maintain a personal ledger containing credit records. Credit records include loan agreements, loan repayments and completed loan records. The second component is a finance dApp capable of reading the private credit ledger and assessing the creditworthiness of the user based on the information within. The risk assessment algorithm sends approval to the lending protocol if the use is found to be credible for a loan application. The lending protocol issues the loan to the wallet of the user and receives payments until the loan is paid off. After the contractual repayment time frame has been passed and if the loan is not fully paid off the lending protocol is able to retrieve personal identity information regarding the user for post-loan management, according to the loan agreement. The third component is a personal identity information retrieval system, consisting of two separate subsystems. Firstly, a temporary identity storage bureau holds the encrypted identity collateral in a distributed storage, like IPFS, and upon request checks for the correct condition to reveal the information to the finance dApp. Secondly, a proxy re-encryption cloud holds the encrypted key to the encrypted identity collateral. Upon request the key is re-encrypted for the public key of the finance dApp, which allows the lending protocol to initiate post-loan management.

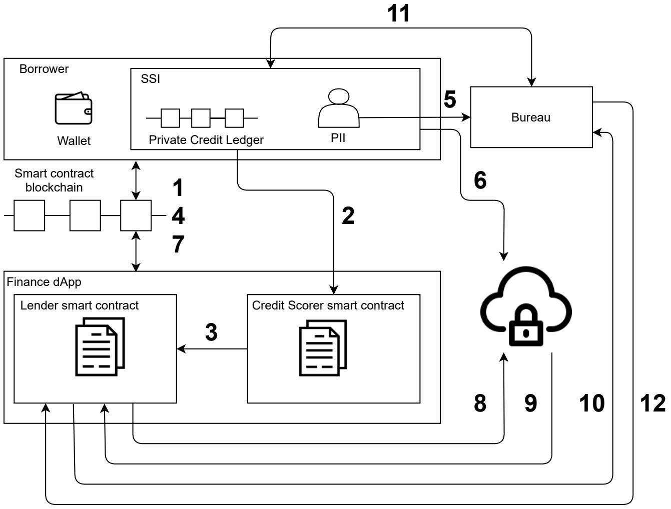

Figure 3: System architecture of our solution

In figure 3 the architecture of the system and the flow between the three components is shown. The description of each step is summarized as follows:

1. The user finds the finance dApp on the public blockchain and requests a loan of a specific size and indicates the use of identity collateral as well as credit history. The finance dApp requests the credit history found on the personal credit ledger.
2. The user accepts the request for the personal credit ledger and sends over the ledger in the form of a verified presentation.
3. Internally, the finance dApp performs analysis of the credit history and is able to verify the records with the respective attestors. A creditworthiness attribute is assigned to the loan request if the user is deemed so.
4. If the credit history is insufficient, the current loan request is denied and the finance dApp might suggest reapplying for a smaller loan or providing different collateral. Otherwise the loan agreement is presented to the user for evaluation, containing interest rate, loan duration and required identity collateral.
5. If the user accepts the agreed terms they must prepare their identity collateral. A symmetric key pair(pk_A, sk_A) is generated for encrypting their their personal identity information. The user then encrypts their identity collateral with the public key pk_A and stores that with the bureau.

[16] https://z.cash/

[17] https://zksync.io/

6. The proxy re-encryption cloud allows the posted identity collateral to be decrypted if that is deemed necessary. The user encrypts the private key pk_A through proxy re-encryption with the public key pk_L of the lending protocol and uploads it to the PRE cloud server.
7. After step 5 and 6, the addresses of the bureau and the PRE cloud server are appended to the loan agreement. Both parties sign and the agreed loan is deposited into the wallet of the user. The issued loan is posted on the private credit ledger as a verified credential signed by the user and the lending protocol. Over the duration of the loan the user must send repayments directly into the address of the lending protocol until the loan is fully paid off, updating the private credit ledger with additional claims. After the loan is completed a credential to creditworthiness is appended to the private credit ledger.
8. In the case of a breach of contract according to the loan agreement an identity collateral retrieval procedure is initiated. The finance dApp requests the decryption key from the PRE cloud by presenting proving a challenge with their private key sk_L.
9. The proxy cloud re-encrypts the cipher text for the lender's public key pk_L and sent it to the finance dApp.
10. To retrieve the identity collateral the finance dApp requests it from the bureau along with a claim that the loan has defaulted.
11. The bureau will contact the user in order to disprove or attest to the claim. If the user is able to present a verified credential to the completed loan the bureau will not send over the encrypted identity collateral.
12. If the default claim cannot be disproved, the loan is assumed default and the finance dApp receives the encrypted identity collateral. The finance dApp will decrypt the received cipher text from the cloud using its private key pk_L and use the obtained symmetric key to decrypt the encrypted identity collateral for post-loan management.

The solution is designed to be protocol agnostic and any lending protocol using the solution should be able to retrieve credit scoring through the credential storage.

5.1 Preparation

In the figures [4-7] a flow diagram is presented that illustrates the interactions between an identity holder and multiple attestors in the SSI environment as well as the interaction between the identity holder and a Risk Assessment Protocol that issues a Credit Score based on the provided claims.

In figure 4 the SSI preperation and credit score application is shown. An SSI holder is able to exchange the legally necessary data with the DeFi protocol to prove its identity as well as the ability to follow up on the repayments for a requested loan. The Lending protocol complies with KYC checks through a fresh KYC-evaluation or inferred KYC history. As KYC is a legal requirement for financial business[10], only users that are able to provide such a credential are permitted into the system.

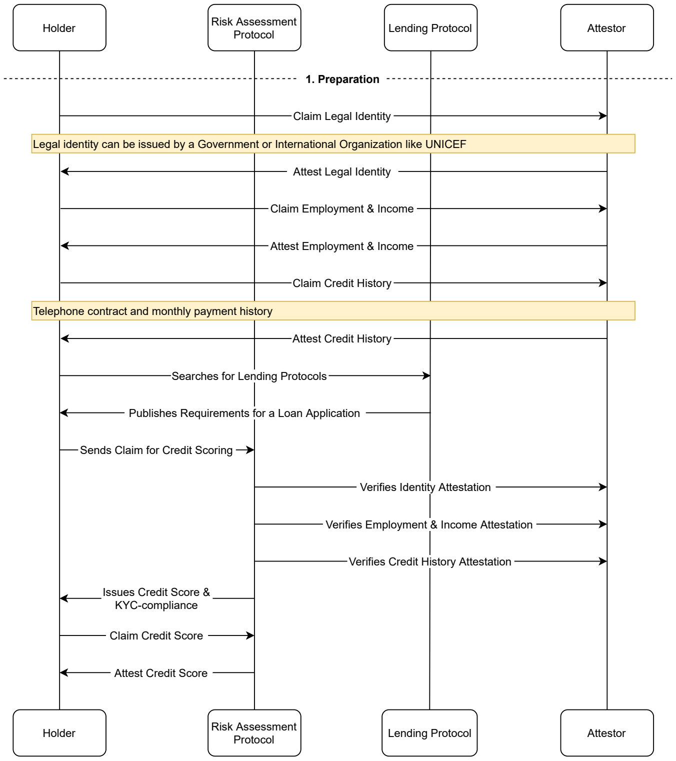
Holder
Risk Assessment Protocol
Lending Protocol
Attestor
1. Preparation
Claim Legal Identity
Legal identity can be issued by a Government or International Organization like UNICEF
Attest Legal Identity
Claim Employment & Income
Attest Employment & Income
Claim Credit History
Telephone contract and monthly payment history
Attest Credit History
Searches for Lending Protocols
Publishes Requirements for a Loan Application
Sends Claim for Credit Scoring
Verifies Identity Attestation
Verifies Employment & Income Attestation
Verifies Credit History Attestation
Issues Credit Score & KYC-compliance
Claim Credit Score
Attest Credit Score
Holder
Risk Assessment Protocol
Lending Protocol
Attestor

Figure 4: Flow diagram of the preparation phase for SSI enabled KYC and Employment status for DeFi lending

5.2 Loan Application

In Figure 5 the loan application flow is shown. Upon request, the identity holder is able to provide an attested Credit Score Claim to the Lending Protocol that implies KYC-compliance. The Lending Protocol verifies that the claim is attested by a trusted Risk Assessment Protocol using its public key. If the provided score is deemed sufficient by the protocol a signed loan agreement is proposed to the holder with loan size, duration and interest rate. The holder then is able to accept or reject the loan agreement. Acceptance requires the holder to send the loan agreement back with its own signature indicating both parties agreement, whereas rejection results in termination of the loan application. Upon receiving an accepted loan agreement, the lending protocol issues the loan to the specified address of the holder. The lending protocol also attests to a credential of the issued loan, that the holder can use as proof to their lending history.

5.3 Post-loan management

In Figure 6 the repayment or defaulting procedure is shown through a flow diagram. The Borrower repays their loan according to the agreed terms, commonly in monthly installments and with a set or variable interest rate. As the loan matures the state of the outstanding debt and repayment history is issued as an updated credential to the Borrower. The payment goes into the smart contract address of the lending protocol. After the loan period is over and the debt is fully paid off, the loan credential state is updated and a successful loan credential is issued. If the borrower does not repay the

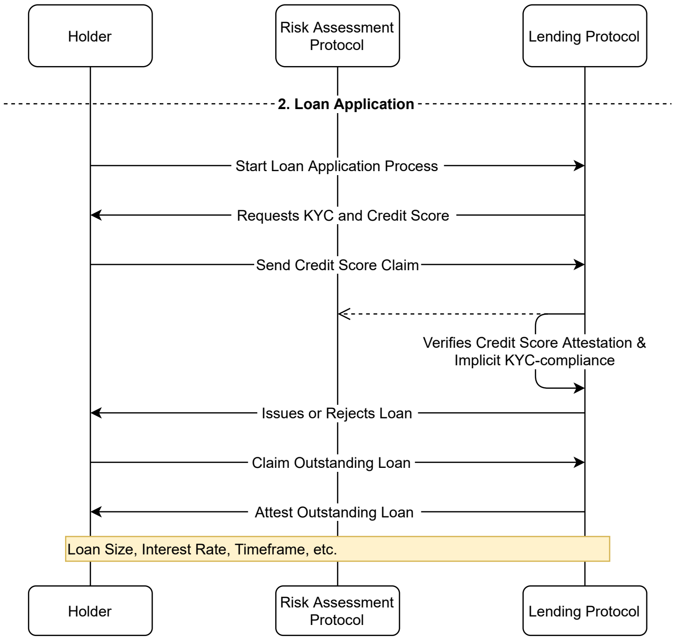

Figure 5: Flow diagram of the loan application phase for SSI enabled KYC and Employment status for DeFi lending

loan at all or partially, then according to the loan agreement a collection procedure is initialized. The Lending protocol updates the state of the loan credential and requests required information of the Risk Assessment Protocol. Upon that request the credit risk protocol verifies a default and issues information gathered in the KYC process.

5.4 Reuse of credit history

In Figure 7 a flow diagram shows the reuse of credentials and faster issuance of new loans. A returning Borrower can reapply for a risk assessment with the Risk Assessment Protocol by sending their accumulated Loan credentials and previously issued Credit Score. The Risk Assessment Protocol verifies the loan credential with the Lender and the Credit Score with the Risk Assessment Protocol. Then a new Credit Score credential is issued to the Borrower, while the old Credit Score is revoked. Upon starting a new Loan Application process the Borrower sends over their Credit Score and Successful Loan history to the Lender. The reuse of historic lending data reinforces a borrower's creditworthiness which in turn institutes them to more favourable interest rates and credit limits.

6 Responsible Research

In regards to the reproducability and related work this paper appropriately cites academic and business sources. Importance to academic literature is proportionate to their position in citation score and accreditation of the authors. Informal sources are hold to lesser standards in nature therefore not relied upon for scientific facts, but instead as indicative of practical implementations. Importantly, due to the rise and fall of decentralized applications, sources related to DeFi protocols apart from white papers, such as blog-, forum posts and web pages are temporary and should be retrieved through internet

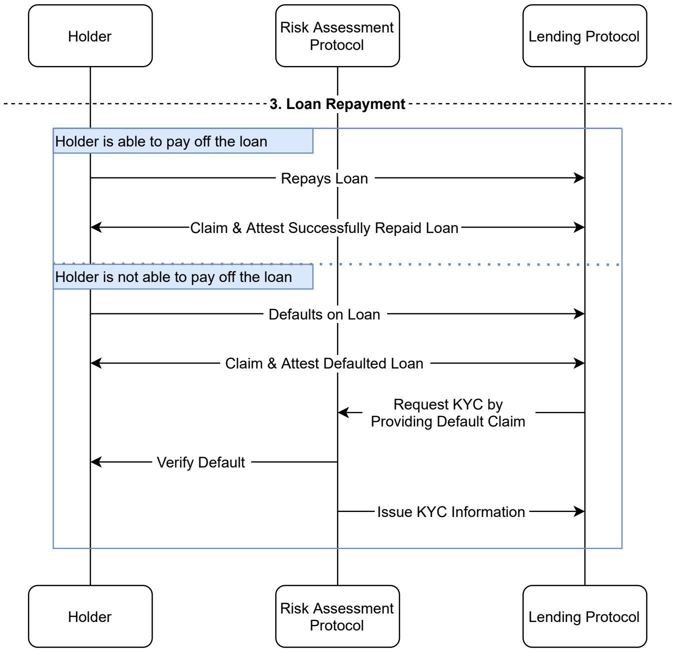
Holder
Risk Assessment Protocol
Lending Protocol
3. Loan Repayment
Holder is able to pay off the loan
Repays Loan
Claim & Attest Successfully Repaid Loan
Holder is not able to pay off the loan
Defaults on Loan
Claim & Attest Defaulted Loan
Request KYC by Providing Default Claim
Verify Default
Issue KYC Information
Holder
Risk Assessment Protocol
Lending Protocol

Figure 6: Flow diagram of the loan repayment phase for SSI enabled KYC and Employment status for DeFi lending

archival services. SSI has been heralded as a privacy preserving solution to digital identity and the SSI design used in this paper adheres to those principles. The legal necessity of KYC procedures in transactions between financial institutions and persons requires legal entities on both sides of the transaction. This implies that a user of the solution has to provide a legal identity through their SSI provider. This legal requirement alienates those that do not posses, either (a.) the ability to prove their identity through a legal identity provider or (b.) a legal identity an sich, due to refugee status or other causes. Decentralized finance is based on permissionless ideals allowing anybody with internet access to participate. Identity collateral in the case of unsecured loans is essentially privacy-sensitive and therefore efforts have been made to delicately address this issue. All personal identity information that users consent to use in the personal identity retrieval system is appropriately encrypted with unique symmetric keys for each user. Storage of encrypted personal identity information and access control of decrypting keys are separated in two distinct systems

7 Conclusions and Future Work

This paper proposes a novel solution to cryptographically secured loans in a decentralized system by presenting a credit history linked to a persistent self-sovereign identity. We identified the limitations of current solutions and bridging between identity claims and pseudonymous credit history and proposed a solution that reintroduces trust only when absolutely necessary. Honest users are able to profit of the ability to borrow without opportunity cost by providing an identity collateral, while lenders are ensured creditworthiness and a backstop in the form of verified personal identity information

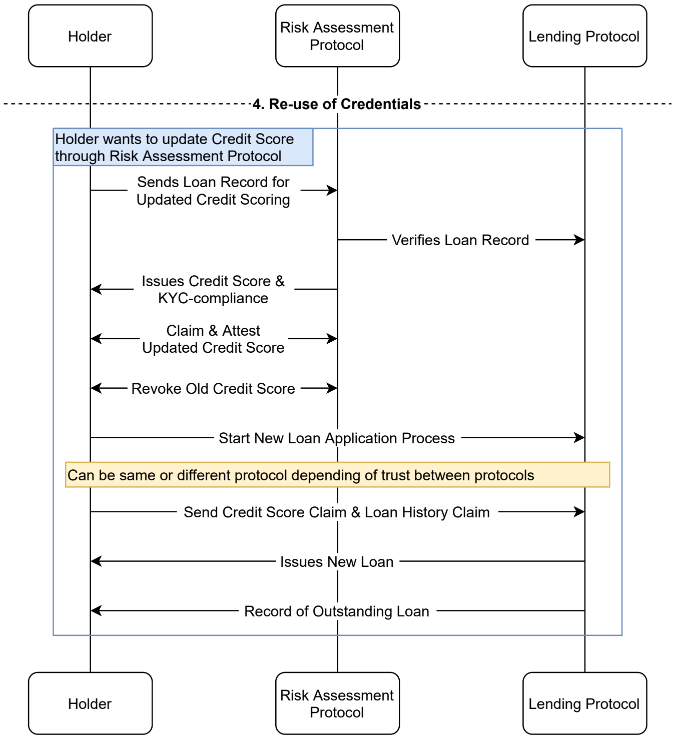
Holder
Risk Assessment Protocol
Lending Protocol
4. Re-use of Credentials
Holder wants to update Credit Score through Risk Assessment Protocol
Sends Loan Record for Updated Credit Scoring
Verifies Loan Record
Issues Credit Score & KYC-compliance
Claim & Attest Updated Credit Score
Revoke Old Credit Score
Start New Loan Application Process
Can be same or different protocol depending of trust between protocols
Send Credit Score Claim & Loan History Claim
Issues New Loan
Record of Outstanding Loan
Holder
Risk Assessment Protocol
Lending Protocol

Figure 7: Flow diagram of the reuse credential phase for SSI enabled KYC and Employment status for DeFi lending

for post-loan management. The price to pay for uncollateralized loans is risking ones identity information equivalent of traditional banking today. Future work should focus on implementing the proposed architecture using a self-sovereign identity solution that allows a user to establish a private credit ledger and a proxy re-encryption algorithm to harness access control over securely encrypted personal identity information.

References

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Business Review, 2008, 21260.

[2] S. Werner et al., Systemization of Knowledge: Decentralized Finance (DeFi), Imperial College London, 2021

[3] M. Bartoletti, J. Chiang & A. LluchLafuente, Systemization of Knowledge: Lending pools in decentralized finance, 2020

[4] D. Wang et al. Towards Understanding Flash Loans and Its Applications in DeFi Ecosystem. ZheJian University, 2020

[5] A. Brauneis, R. Mestel, R. Riordan & E. Theissen, How to measure the liquidity of cryptocurrency markets?, Journal of Banking & Finance, 2021.

[6] N. Carter & L. Jeng. DeFi Protocol Risks: the Paradox of DeFi, June 14, 2021. "Regtech, Suptech and Beyond: Innovation and Technology in Financial Services," editors, Coen, Bill and Maurice, Diane. RiskBooks – forthcoming 3Q 2021., Available at SSRN: https://ssrn-com.tudelft.idm.oclc.org/abstract=3866705

[7] T. Ziegler et al. The 4th European Alternative Finance Benchmarking Report

[8] R. Todd, The State of the Crypto Credit Ecosystem. The Block Research, May 2021. accessed through: https://www.theblockresearch.com/the-state-of-the-crypto-credit-ecosystem-99536

[9] C. Harwick & J. Caton, What's holding back blockchain finance? On the possibilities of decentralized autonomous finance, The Quarterly review of Economics and Finance, 2020.

[10] EU Parliament and Council Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. OJ L141/73, 2015

[11] FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html, 2012-2020

[12] F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74. https://doi.org/10.20955/r.103.153-74

[13] Baars, D. S. Towards self-sovereign identity using blockchain technology. MS thesis. University of Twente, 2016.

[14] Allen, C. The Path to Self-Sovereign Identity. 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[15] D. Harz et al., Balance: Dynamic Adjustment of cryptocurrency deposits, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1485 1502, 2019

[16] D. Harz et al., Promise: Leveraging future gains for collateral reduction, IACR Cryptol, vol. 2020, p. 532, 2020

[17] R. Berkun & I. Perez. Teller Protocol: An algorithmic credit risk protocol for decentralizing lending. Whitepaper, 15 July 2020

[18] R. Berkun & C. Lee. Stratosphere: A Distruted Cloud Network for Decentralized Application Scalability.

[19] https://teller.gitbook.io/teller-docs/protocol-1/faq

[20] Kiva https://www.hyperledger.org/learn/publications/kiva-case-study

[21] HyperLedger Indy https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md

[22] Colendi Technical Paper

[23] Y. Chen et al. Research on the Secure Financial Surveillance Blockchain Systems. International Journal of Network Security, Vol. 22, No. 4, pp 708-716, July 2020

[24] C. Dong, Z. Wang, S. Chen & Y. Xiang. BBM: A Blockchain-Based Model for Open Banking via Self-Sovereign Identity. ICBC 2020, LNCS 12404, pp. 61-75, 2020. Springer Nature. Swinburne University of Technology, Melbourne. 2020

[25] Jeyasheela Rakkini M.J., Geetha K. (2021) Blockchain-Enabled Microfinance Model with Decentralized Autonomous Organizations. In: Smys S., Palanisamy R., Rocha Á., Beligiannis G.N. (eds) Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 58. Springer, Singapore.

[26] H. Wang, C. Guo & S. Cheng. LoC - A new financial loan management system based on smart contracts. Future Generation Computer Systems 100 (2019) pp. 648-655

[27] V. Hasija et al. Secure Lending: Blockchain and Prospect Theory-Based Decentralized Credit Scoring Model. IEEE Transactions on Network Science and Engineering, Vol. 7, No. 4, October-December 2020

[28] B. Sharma, R. Halder and J. Singh. Blockchain-based Interoperable Healthcare using Zero-Knowledge Proofs and Proxy Re-Encryption. In 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS). 2020 IEEE. https://doi.org/10.1109/comsnets48256.2020.9027413

[29] MyKey https://mykey.org/keyid

[30] Metamask metamask.io

[31] Bloom bloom.co

[32] J. Leimgruber, A. Meier, J. Backus, Bloom Protocol, Decentralized credit scoring powered by Ethereum and IPFS. 27 January 2018. accessed through: https://hellobloom.io/whitepaper.pdf

[33] uPort/Serto serto.id

[34] w3c DID specification https://w3c.github.io/did-core/

[35] Sidetree https://identity.foundation/sidetree/spec/

[36] ION https://github.com/decentralized-identity/ion

[37] A. Tobin & D. Reed, The inevitable rise of Self-Sovereign Identity, White paper, 2017.

[38] I. Damgård et al. Balancing Privacy and Accountability in Blockchain Identity Management. Cryptology ePrint Archive, Report 2020/1511, 2020

[39] Q. Stokkink & J. Pouwelse, Deployment of a blockchain-based self-sovereign identity. 2018 IEEE conference, 2018

[40] P. Zimmermann. Why i wrote pgp. PGP User's Guide, 1991

[41] Sivakumar, P., & Singh. Privacy based decentralized Public Key Infrastructure (PKI) implementation using Smart contract in Blockchain. technical report. 2017

[42] Dötling N. and Nishimaki R. Universal Proxy Re-Encryption. Public-Key Cryptography - PKC 2021. Springer. 2021

[43] M. e. a. Blaze, "Divertible protocols and atomic proxy cryptography," in Advances in Cryptology — EUROCRYPT'98, K. Nyberg, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 127–144.

[44] Goldreich, O., Micali, S., and Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. Journal of the ACM (JACM), 38(3):690–728.

[45] Kulabukhova, N. V. (2019, January). Zero-knowledge proof in self-sovereign identity. In Proceedings of the 27th International Symposium Nuclear Electronics and Computing (NEC'2019) (pp. 381-385).

[46] R. Chotkan, Industry-Grade Self-Sovereign Identity DRAFT. MSc Thesis. TU Delft, 2021

[47] AAVE protocol whitepaper, AAVE, 2021

[48] R. Leshner & G. Hayes, Compound: The Money Market Protocol, Whitepaper, 2019

[49] N. Jain, T. Agrawal, P. Goyal, V. Hassija, A Blockchain-Based distributed network for Secure Credit Scoring, 10‘9 5th International Conference on Signal Processing, Computing and Control (ISPCC), 2019, pp. 306-312, doi: 10.1109/ISPCC48220.2019.8988510

[50] MemberPass https://www.hyperledger.org/learn/publications/culedg
case-study