Privacy Considerations for a Decentralized Finance (DeFi) Loans Platform

Janka Hartmann and Omar Hasan

Department of Computer Science, INSA Lyon, Villeurbanne, 69621, France.

Contributing authors: janka.hartmann@mailbox.org; omar.hasan@insa-lyon.fr;

Abstract

There are many Decentralized Finance (DeFi) Peer-to-Peer (P2P) lending platforms that offer users to obtain a loan by committing a collateral or by calculating a "credit score", which is based on factors such as the users' credit history. However, the requirements of collateral and credit history are quite burdensome for some users. Nowadays, with more than 55% of the global population using social media, there is a lot of publicly available personal data [1]. This data could be used as an alternative risk mitigator for lending. There are many inferences that can be drawn from the users' social media accounts about their professional behavior and reliability, allowing us to derive the users' social trustworthiness. We propose to calculate a "social score" based on the social media data of a user. Our contribution is to develop an Ethereum blockchain-enabled fully decentralized lending platform that relies on this score. This platform could give users a chance for a loan even if they do not have a collateral or a sufficient credit score. Furthermore, we discuss privacy considerations for our platform and present an enhanced version that protects the borrower's privacy.

Keywords: blockchain, Ethereum, social capital, lending, finance, P2P, privacy, zero-knowledge proof

Declarations

Funding

Not applicable.

Informed consent

Not applicable.

Ethical statement

The authors declare no conflict of interest.

Author contribution

All authors contributed equally to this work.

Data availability

The dataset used for the current study is available in the Stanford Network Analysis Project (SNAP) repository, https://snap.stanford.edu/data/ego-Facebook.html. The dataset is called "Social circles: Facebook" [2].

1 Introduction

The concept of Decentralized Finance (DeFi) promotes an open financial system where financial services can be provided and accessed without dependence on intermediaries or central authorities. Peer-to-Peer (P2P) lending is one of the main financial services that can be enabled by DeFi technologies. In this work, we look at how social

network data can be used to support peer-to-peer lending while taking privacy considerations into account [1, 2].

Peer-to-peer lending allows a borrower to receive a loan directly from a single or multiple individual lenders. The first peer-to-peer lending platform Zopa [3] went online in 2005. The peer-to-peer lending market has been continuously growing since then and is predicted to keep growing in the future [4]. Some other well known P2P lending platforms are CoinLoan [5], Inlock [6], Prosper [7], and Lending Club [8]. Peer-to-peer lending has several advantages in contrast to traditional lending. It dispenses with middlemen such as financial institutions. The lending platform itself sets the conditions and enables the transactions. Not having middlemen saves time and money, which often allows the platform to offer better rates.

An additional development in recent years is that peer-to-peer lending platforms are based on blockchain and are using smart contracts. This development brings more trust and transparency. This type of lending is fully in line with the concept of decentralized finance. However, since there are no middlemen verifying a potential borrowers' financial situation, they need to prove to the lenders that they are credit worthy. Loans can be secured or unsecured. They are received by either depositing a collateral or by calculating a credit score to prove one's creditworthiness.

1.1 Secured Lending

The term "secured lending" describes a way of lending, where the loan is secured with a collateral. A collateral is a valuable asset (for example, a mortgage on the borrower's house, investments in cryptocurrencies, etc.) which the borrower has to give as insurance for the loan. After receiving the loan, the borrower has to pay back the money within a certain time. If the borrower is unable to pay, the debt is deducted from his collateral. Secured lending carries an element of risk for the borrower: If he cannot pay back the money, he loses his asset. Moreover, the borrower needs to be in possession of a suitable asset in order to qualify for a loan. The lender on the other hand is promised to get his money back. He is therefore often willing to offer better interest rates, which can be an advantage for the borrower in this kind of lending.

1.2 Unsecured Lending

Unsecured loans or personal loans work without a collateral. Collateral has two main problems: Firstly, people may not trust in the lending platform enough to deposit their asset. Secondly, people do not always have the money or property required for a collateral. They can have a good income and be a reliable person but without a collateral they might still not be qualified for a secured loan. Instead of taking a collateral as insurance, unsecured loans rely on a creditworthiness system, which is mostly based on a "credit score". A well-known credit score is the FICO (Fair Isaac Corporation) score [9]. It determines the creditworthiness of a potential borrower by using a fixed formula, which takes into account aspects such as the borrower's payment history, available credit and age. A penalty has to be paid if the monthly payment is not balanced on time. When the borrower defaults paying back his loan, he loses points of his credit score, but not a collateral. Therefore, from the borrower's point of view, unsecured loans are less risky, but can be linked to higher interest rates. A common example for unsecured loans are student loans.

1.3 Peer-to-Peer Lending

In peer-to-peer lending, there exist secured loans as well as unsecured loans. However, while in traditional lending there is mostly some kind of financial institution participating in the process, peer-to-peer lending offers borrowers and lenders to connect directly without such an intermediary. This can translate into lower or no fees and there is no longer a single point of failure. However, since there is no borrower creditworthiness evaluation carried out by a third party, the individual lender himself is responsible for determining whether a person can be trusted to pay back their debts. Peer-to-peer lending platforms are online platforms that offer to match people that want to lend money as a form of investment with people who want to borrow money. A "peer" can also be a company or a group that is in need of a loan. An example of a loan to an individual could be a payday loan, whereas companies might need a loan for commercial reasons or to expand their business.

1.4 Our Approach

The goal of this work is to develop a new approach to calculate the borrowers' trustworthiness based on their social capital, which does not depend on a collateral or the credit history of the user. This approach can stand on its own or it can be used in addition to traditional concepts such as collateral and credit score. The objective is to minimize the risk that the borrower defaults on the loan. It would give those users a chance for a loan who do not have a high enough credit score or the resources to deposit a sufficiently valuable collateral. This approach is based on the "social capital" theory. In this work, we develop a prototype of a decentralized finance peer-to-peer lending platform built on the Ethereum blockchain. The creditworthiness of the users on this platform is represented by a social score, which is calculated by analyzing the users' social media accounts.

There is a large amount of personal data that is available on social network accounts of many people. In the subsequent sections, we discuss how this data can be used to compute the social score of a user. The available data includes biographical information such as name, email address, date of birth, etc., as well as social information such as the number of followers or friends, shared posts, etc. Moreover, in case a user has multiple social network accounts, the information available on different accounts can be compared and co-related to derive inferences about the user as well. In view of "social capital" theory, this multitude of information could portray the trustworthiness of a user, which we could use as an indicator of the user's disposition to repay loans.

We note that using personal information leads to privacy concerns. Therefore, in this work, one of our main objectives is to develop a privacy-preserving loans platform. This privacy-preserving platform aims to prevent disclosure of personal information such as the user's name, email address, date of birth, precise number of friends, etc. In order to achieve privacy, we develop mechanisms using cryptographic building blocks such as homomorphic cryptosystems, zero-knowledge proofs, and cryptographic hash functions.

1.5 Contributions

This work makes the following contributions:

- A new approach to calculate the users' trustworthiness on peer-to-peer lending platforms using the information that can be retrieved from the users' social network accounts instead of relying on collateral and credit scores that can be problematic for the users.
- A brief analysis of the various types of lending and a look at their advantages and disadvantages.
- A description of some of the popular existing online peer-to-peer lending platforms and discussions on how they operate with or without collateral.
- The proposal of an enhanced version of the lending platform that takes privacy considerations into account by using cryptographic building blocks such as zero-knowledge proofs and cryptographic hash functions.
- The development of a prototype of an Ethereum decentralized application that implements the proposed social score formula in a smart contract.
- Quantification of the amount of Ethereum gas that is consumed by the deployment of the smart contract.
- Experiments on a real social network dataset that demonstrate how we can use analysis of social network data to determine optimal thresholds for a platform in production.

1.6 Outline

In Section 2, an introduction to three successful peer-to-peer lending platforms and their methods to ensure the borrowers' creditworthiness is given. In Section 3, we present the fundamentals of the social capital theory. In Section 4, the idea developed in this paper based on the calculation of a social score is presented. The implementation details of a prototype are discussed in Section 5. In Section 6, we discuss privacy considerations for our lending platform and propose a solution for preserving the privacy of borrowers. Section 7 comprises of the evaluation details. This is followed by the conclusion.

2 Related Work

In this section, we describe three existing online peer-to-peer lending platforms. CoinLoan [5] and

Inlock [6] both offer secured loans whereas Prosper [7] offers personal loans. The fundamental principle is that one peer lends a loan and another peer borrows a loan. All three platforms include interest fees, which the borrower has to pay to the lender and an origination fee, which the borrower pays to the platform for using the service.

2.1 CoinLoan

CoinLoan [5] is a peer-to-peer platform founded in 2017. The advantage of borrowing money with CoinLoan is to get a loan right away without having to provide anything except for a collateral in cryptocurrency. The collateral amount, the interest rate and the origination fee are calculated from the user's inputs. The borrowing money function on CoinLoan is only useful for people owning cryptomoney. Moreover, once a user receives a loan, his collateral is blocked until he has paid off his debts. During this time, the user is not able to sell the deposited cryptocurrency, which they might want to do in case the cryptocurrency is facing heavy depreciation. If the user does not pay back on time, the owed amount will be taken from his deposit of cryptomoney.

2.2 Inlock

Inlock [6] is another peer-to-peer lending platform that was founded in 2017. Again, there are no options to prove one's trustworthiness other than to give a collateral. The collateral has to be paid in the form of cryptomoney. Inlock currently supports only four cryptocurrencies: Bitcoin, Ether, Litecoin and Binance Coin. There is a 110% over-collateralization rate along with a universal collateral termination level. Once the collateral decreases below that level, the debts will automatically be paid off by Inlock using the deposited collateral. Thus, the user has to be careful and keep an eye on falling market values of the cryptocurrency.

2.3 Prosper

Prosper [7] is a peer-to-peer lending platform that was founded in 2005. Unlike Inlock and CoinLoan, it does not offer secured, but only personal and hence unsecured loans. Although the user has to give personal data, applying for a loan is a simple and quick process. Since there is no collateral, users do not need to deposit anything and therefore they do not risk to lose their collateral. On the other hand, penalty fees can rise quickly. For not paying back on time, the borrower has to pay USD 15 or 5% of the outstanding debts. They also lose credit score points. The origination fee is significantly higher than it is on other lending platforms such as CoinLoan. Prosper is also restricted in the kinds of loan they offer. As an example, they exclude student loans and other educational loans.

3 Social Capital

We now introduce a concept on which our proposed score is based. According to Rene Dubos in his book "Social Capital: Theory and Research" the "premise behind the notion of social capital is rather simple and straightforward: investment in social relations with expected returns" [10]. He gives four reasons for why "embedded resources in social networks will enhance the outcome of actions" [10]. Firstly, connections can help to get information and information can translate into opportunities. A good example where social connections are often useful is job hunting. Secondly, Dubos claims that having social connections may also have a positive impact on decisions involving the individual, such as discussions about promotions. The decision making process can be strongly influenced by a person putting in a good word for the individual. Thirdly, he claims that companies might value a person's social capital on top of his personal capital. "The individual can provide "added" resources beyond his / her personal capital, some of which may be useful to the organization" [10]. The fourth reason Dubos states is that being well connected provides both "emotional support" [10] and "public acknowledgment of one's claim to certain resources" [10].

Robert Putnam claimed that "economic performance as a whole is better in well-connected societies than in poorly connected ones" [11]. This claim triggered many studies on the topic. A Swedish study on unemployed Swedes resulted in the conclusion that "network size had a considerable positive impact on the likelihood of finding work, far outweighing the official employment agency" [11]. Another study, performed in Germany, revealed "that engagement in a range of social activities is positively linked with job-finding among the unemployed" [11].

In this paper, we aim to use social media network information of a person to determine their social capital and to draw conclusions about possible connections in other areas like financial behavior. "The central idea of social capital is that social networks are a valuable asset" [11]. Being well-connected on social media brings advantages similar to real world connections. It helps the user to stay informed and to find possible opportunities. Further, a social media entry, such as a picture about the individual participating in a certain event, could help the individual to receive recognition. It could be a conversation opener and enable them to establish new contacts. The contacts might be useful and might put in a good word for the individual at some point.

Another widely investigated and supported claim of Putnam is that "higher levels of social capital . . . translate into lower levels of crime" [11]. Further studies have demonstrated that there is higher criminality in neighborhoods where people live rather anonymously and do not maintain contact with their neighbors [11]. Social connections have a large impact on people's well-being, but there seem to be more benefits. "There appear to be clear and often strong positive links between social capital and educational attainment, economic success, health and freedom from crime." [11].

4 Our Decentralized Lending Platform

In this section, we propose a new approach for decentralized lending: unsecured loans based on the users' social score, instead of their credit score.

4.1 Creditworthiness Depending on a Social Score

The social score presented in this paper is calculated based on one or several social media accounts of the user. Our algorithm analyzes the user's accounts to determine his personal social score. The algorithm is based on six hypotheses that estimate the trustworthiness of a user.

Hypothesis 1: Users who add their social media account have less to hide

Our social media account says a lot about us: who are our friends, what are our likes and dislikes, what are our ambitions, etc. The social media account may also provide some personal data, such as our age, current location, and our profession. Most people are aware of the fact that their social media account can reveal a lot of information. Therefore, if they have something to hide, for example a bad habit like gambling, they will hesitate to connect their social media to a peer-to-peer lending platform, that calculates a score derived from their social media information. As we saw in the neighborhood example [11] given in the subsection about social capital: Criminality is lower when anonymity is absent and people are part of a community. Based on this theory, the risk to default may be lower for users who add their social media accounts and therefore lose their anonymity. As a result, one may assume that users who disclose their social media account have less to hide and may therefore be considered trustworthy.

Hypothesis 2: The more the user is willing to disclose about himself, the more trustworthy he is

There are a lot of social media platforms these days. Currently, three important platforms are Facebook, Instagram and LinkedIn. All three platforms together cover a wide range of information about a user, which include both private and professional information. The more accounts from different platforms a user is willing to disclose, the more information about himself he is ready to provide. By giving this information about himself, the user proves once again his willingness to give up his anonymity. As already mentioned in hypothesis 1, we assume that users who give up their anonymity have less to hide and may therefore be considered trustworthy.

Hypothesis 3: Trustworthy users have authentic social media profiles

To avoid that users simply disclose some accounts they just created or some fake account for the pure purpose of improving their social score, the authenticity needs to be checked. There are many indicators when it comes to identifying fake accounts. These include posting original pictures, having a significant number of mutual friends and followers, and having a non-recent date of creation of the account. For example, on Instagram, fake

accounts do not have a lot of mutual friends and typically follow more people than they are followed by. According to [12], fake profiles have around 30 times as many friends as followers.

Hypothesis 4: The bigger the social network and activity, the more credit worthy is the person

The Swedish study concluded that "network size had a considerable positive impact on the likelihood of finding work" [11]. Therefore, users with more social contacts and thus more followers and friends on social media, are less likely to get stuck in unemployment. Also, the well-being of people strongly depends on their social network and on how connected they are. The more social activity a user has, the higher is his social capital. "There appear to be clear and often strong positive links between social capital and educational attainment, economic success, health and freedom from crime." [11]. Therefore, more friends and connections as well as posts lead to a higher social score.

Hypothesis 5: People who make truthful statements are trustworthy

"Interpersonal trust is fundamental for the effective functioning of social interactions as well as of society as a whole. It has been found to be related to many societal outcomes such as lower corruption perception" [13]. Trust is fundamental in peer-to-peer lending as well. A lender needs to trust in the borrower's good will to pay back the loan. To be trusted to get a loan, a user's honesty is tested. Therefore, before connecting with the social media accounts, the user will be asked to give three personal information: the full name, date of birth, and email address. When connecting the social media accounts, this information will be compared. If the information are corroborated by multiple social media accounts, this is taken as an indication of the user's honesty and openness.

Hypothesis 6: Consistency is a sign for stability

If a user agrees to connect multiple social media accounts, the data of these accounts can be checked for consistency. Being friends with the same people and showing a similar profile on different social media platforms indicates that these accounts represent one and the same person.

4.2 Social Scoring in Peer-to-Peer Lending

The mentioned hypotheses need to be converted into variables and formulas that we can calculate our social score with. Each of those variables will have an impact on the final social score. The final social score will be received by calculating the average of the individual social media platforms accounts plus a bonus for disclosing more social media accounts.

$$DISC_x = OPEN_x * AUTH_x \tag{1}$$

The first variable is $DISC_x$, which stands for disclosure of the user's account from the platform x. Here, x could be for Facebook, Instagram, or LinkedIn. The variable can vary between zero and one, depending on the user's openness to disclose his social media account x and that account's authenticity. The $OPEN_x$ variable can only take the value one or zero. If the account x is disclosed by the user, $OPEN_x$ equals 1, whereas if the user doesn't disclose his account x, the $OPEN_x$ variable is zero and therefore $DISC_x$ equals 0. The $AUTH_x$ variable describes the authenticity of the disclosed account x. It varies between 0 and 1. It is zero, if an account contains no information at all or if it is classified as fake. It is one when an account is authentic. The variation between 0 and 1 is incremental according to a value pre-defined by the platform operator. For example, one could assign 0.2 for the first 100 followers / friends, 0.4 for the first 1000, and so on. The maximum value of $DISC_x$ is therefore one if the user discloses his account x ($OPEN_x = 1$) and the account is classified as authentic ($AUTH_x = 1$).

The precise function for computing $AUTH_x$ is to be defined by the platform operator. The value of $AUTH_x$ is computed based on the number of friends of a user. In Equation 2, we give an example of the function that could be used, where $f =$ the number of friends of the user.

$$AUTH_x = \begin{cases} 0 & \text{if } f < 100 \\ 0.2 & \text{if } f \geq 100 \text{ and } f < 1000 \\ 0.4 & \text{if } f \geq 1000 \text{ and } f < 10000 \\ 0.6 & \text{if } f \geq 10000 \text{ and } f < 100000 \\ 0.8 & \text{if } f \geq 100000 \text{ and } f < 1000000 \\ 1 & \text{if } f \geq 1000000 \end{cases} \quad (2)$$

We present a function below to calculate the Social Score of a person, which is abbreviated by SC_x.

$$SC_x = DISC_x * HON_x \quad (3)$$

HON_x is short for honesty. The entered user data on our peer-to-peer lending platform consists of the name, the email address and the date of birth. This data is compared to the data available on the social media platform x. If none of the information match, HON_x equals zero. If only the email address matches, the honesty-value is 20. The same applies if only the name matches. A matching birth date adds 10 to HON_x. The maximum value for HON_x is 50 when all three information match.

$$bonus = n * 2 * CONS \quad (4)$$

A bonus is given on the final social score depending on the number of disclosed accounts n. The maximal number of disclosed accounts is 5. The variable $CONS$ stands for consistency. It varies between 0 and 5 and conveys the concordance between the different disclosed accounts. When the same username is used among the social media accounts of the different portals, $CONS$ increases by 2. We increase the bonus by 2 again if the email address matches. For the same birthday information, the bonus is increased by 1 for consistency. The maximal number of points reached by the bonus is therefore 50.

$$SC = \frac{(SC_1 + SC_2 + ... + SC_n)}{n} + bonus \quad (5)$$

The final equation is composed of the sum of the single social score's average and the bonus. The complete formula would look like this:

$$SC = \frac{(O_1 * A_1 * H_1 + ... + O_n * A_n * H_n)}{n} + n*2*C \quad (6)$$

In this equation, O is short for open [OPEN], A stands for authenticity [AUTH], H for honesty [HON] and C for consistency [CONS]. If the user does not disclose any accounts, every $OPEN$ variable and n is zero. No social media based observation can be made as no data can be accessed. Since all the partial terms $SC_1, SC_2, ..., SC_n$ contain a multiplication by zero, they all end up having the value 0. For $n = 0$, the bonus equals zero, and as a consequence, the final social score (SC) will add up to zero as well. Table 1 summarizes the correspondence of the variables in the social score formula to the hypotheses listed in Section 4.1.

Hypothesis	Variable	Description
1	$OPEN_x$	Whether a social media account on the platform x is disclosed or not.
2	n	The number of accounts disclosed.
3	$AUTH_x$	The authenticity of the disclosed account on platform x.
4	$AUTH_x$	The value of the authenticity variable reflects the size of the user's network on platform x.
5	HON_x	The honesty of the user, determined by comparing the information declared by the user and the information retrieved from the user's account on platform x.
6	$CONS$	The consistency of information between the different disclosed accounts.

Table 1 Correspondence of the variables in the social score formula to the hypotheses listed in Section 4.1.

The highest social score that can be achieved this way is 100 and the lowest is 0. Note that a low social score in this system does not mean that the user is guaranteed to have bad intentions or cannot be trusted. It could also mean that the user is not very active on social media. In any case, it means that the user did not reveal much about himself and that his social media accounts do not give us sufficient reason to trust him. In this situation, the user may obtain loans through traditional lending mechanisms such as using a collateral or his credit score.

5 Implementation

The information that is entered by the user and the calculated social score are saved on the

blockchain. This information includes the user's name, email address, date of birth, loan amount, and the social score. The clear disadvantage of saving this information on a public blockchain is lack of the user's privacy. As we discussed in our conference paper [14] that described only the non-privacy-preserving version of our lending plaform, future work should address this problem of user privacy. In Section 6 of this paper, we do indeed present an enhanced version of our platform that takes privacy considerations into account. For the current prototype, we consider that the data will be publicly accessible. In a future iteration of the prototype, we may store only the less sensitive information on the blockchain, for example, only the loan amount and the social score. The changes required in the code would be minimal since $setInfos$ is the only function that would need to be adapted.

5.1 Tools and Technologies

We decided to develop this implementation on an Ethereum test network. As stated in [15], the Ethereum test network ("testnet") simulates Ethereum, which gives the developers a chance to deploy and test Ethereum projects without getting any real assets involved. The testnet allows developers to easily obtain tokens and Ether for test purposes, which carry no financial value. This makes it possible to test a project with simulated tokens and Ether instead of using expensive valuable assets. A guide to using an Ethereum test network is provided by Hayes [15].

We connect to the Ethereum test network using Ganache (www.trufflesuite.com/ganache). Ganache is a tool that is used for setting up a local Ethereum blockchain. The smart contracts for this project are written in the programming language Solidity on the Ethereum IDE Remix (remix.ethereum.org). Solidity is a statically-typed programming language that allows developing smart contracts for Ethereum. Remix IDE is an open source web-based platform, which has a plugin architecture that promotes extensibility. Remix IDE provides several tools for all the steps required for smart contract development with the Solidity language.

To connect our smart contract with the Ganache blockchain, we use MetaMask (metamask.io). MetaMask is an Ethereum wallet. The wallet tries to simplify user experience for accessing decentralized applications (dApps) deployed on Ethereum. MetaMask can be installed as a browser extension. This allows it to provide a user-friendly interface for sending and receiving Ether.

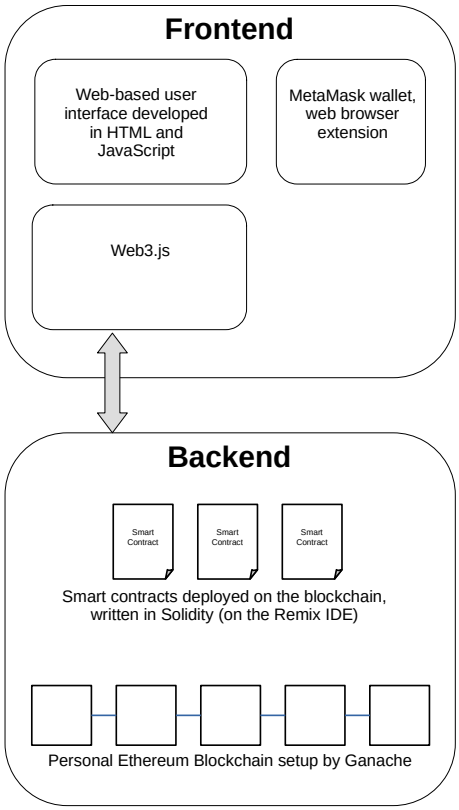

Fig. 1 Architecture of the prototype implementation.

For the frontend of the implementation, we use HTML and JavaScript. The frontend connects to the backend and therefore we test our blockchain by using the library Web3.js (web3js.readthedocs.io). Web3.js enables interaction with a local or remote Ethereum node using HTTP as well as some other protocols.

The architecture of the prototype implementation is shown in Figure 1.

5.2 Smart Contract Implementation and Ethereum Gas Usage

According to [16], a smart contract is a program that is stored on a blockchain and runs when certain predetermined conditions are met. A smart

contract is used to automate and enforce the execution of an agreement that has been made beforehand between the participants of the smart contract. The smart contract guarantees that the outcome of the execution will satisfy the agreed upon conditions. Moreover, the execution of the smart contract does not require the involvement of any intermediaries or trusted third parties.

On the Ehtereum platform, "gas" is a measure of the computational resources that are needed for the execution of a function of a smart contract. Executing a function requires payment of the gas fees determined for that function according to the computational resources that it would use.

Once the smart contract is deployed, one can use the functions within this smart contract while interacting with the blockchain. By calling a function in the smart contract that writes on the blockchain, for example the "setInfos" function, a block is mined and therefore gas must be payed. However, when one of the view-functions is called, no gas needs to be payed and no new block is mined on the blockchain. The "setInfos" functions is called only once when a person registers for the first time.

One main advantage of a smart contract is that the calculations performed are transparent and everybody can have trust in the calculated score. The smart contract calculates the score and then stores it in the blockchain by itself, without the intervention of any outside code. This way, everybody can trust in the process, including the user himself, and nobody can manipulate it. Figure 2 shows the listing of the functions in the smart contract implemented in Solidity.

Five of the functions in the smart contract write to the blockchain and therefore cost gas. The other functions are read- or view-only functions. The smart contract is deployed and written on the blockchain, which costs ether. The gas cost is 2141686. However, the smart contract only has to be deployed once. The functions within the smart contract, which cost ether because they write on the blockchain, are also called only once. This is done during the registration process. Not all of the functions are necessarily called. If the user does not connect his Facebook account, the function "calculateFBScore" is not called. The same is true for connecting the Instagram account and the LinkedIn account. If only one account is connected, there is no bonus added on top of the social score and as a consequence, the "calculateBonus" function is not called. The only gas costing function that is always called, is the "setInfos" function.

We also employ a helper function to compare strings. Further, we have one calculation function for each social media network and one function to calculate the bonus. None of the functions has a return value. They all work directly on the globally saved "socialScore" variable.

6 Privacy Considerations

As we have seen in Section 4.2, the initial version of our lending platform does not take the privacy of the borrower into account. A significant amount of personal information needs to be disclosed by the borrower in order for the lender to compute his social score. In this section, we discuss privacy considerations for our lending platform. We begin by looking at the private details that are divulged on the initial version of the platform. We then state our objectives for an enhanced privacy-preserving version of the platform. After that, we describe some cryptographic building blocks that we use. We then introduce our proposed measures based on the cryptographic building blocks to ensure the privacy of the borrower on the platform. We end this section with an overview of the security of our proposed privacy-preserving measures.

6.1 Analysis of the Disclosure of Private Information

We analyze what private information is revealed about the borrower for the computation of the various variables by the lender.

- $DISC_x$ is computed as a function of $OPEN_x$ and $AUTH_x$. Let's first look at the information revealed for $OPEN_x$. In order for the lender to equate $OPEN_x = 1$, the borrower gives access to his account on the social network x. This reveals the identity of the account as well as the content of the account to the lender.
- The $AUTH_x$ variable is computed as a function of the number of friends or followers of the borrower on the social network account x. Therefore, the borrower is expected to divulge the precise number of his friends or followers to the lender.

```
 6 contract Register {
 7     string private info;
 8     string private name;
 9     string private email;
10     string private birthday;
11     uint private loanAmount0;
12     uint private socialScore = 0;
13
14     function compareStrings(string memory a, string memory b) public vi
17
18     function calculateFBScore(string memory firstName, string memory la
76
77     function calculateInstaScore(string memory firstName, string memory
276
277    function calculateLinkedInScore(string memory firstName, string mem
476
477
478    function calculateBonus(uint connectedAccounts, string memory faceb
489
490    function setInfos(string memory _info, string memory _name, string
497
498    function getInfo() public view returns (string memory) {...}
501
502    function getName() public view returns (string memory) {...}
505
506    function getMail() public view returns (string memory) {...}
509
510    function getBirthday() public view returns (string memory) {...}
513
514    function getLoanAmount() public view returns (uint) {...}
517
518    function getSocialScore() public view returns (uint) {...}
521
522 }
```

Fig. 2 Overview of the smart contract functions used in our implementation of the proposed system.

- SC_x is computed as a function of $DISC_x$ and HON_x. In order for the lender to compute HON_x, the borrower must provide personal information such as his name, email address, and date of birth on the lending platform. The lender then also accesses the corresponding information on the user's social network account x for the purpose of matching the two sets of information.
- The variable *bonus* is computed as a function of the variables n and $CONS$, where n is the number of social network accounts disclosed. In order to compute $CONS$, the lender accesses the content of n social network accounts of the borrower for checking the consistency of information among those accounts.
- SC is a function of the variables $SC_1 \ldots SC_n$, n, and *bonus*, which have all been discussed above.

6.2 Privacy Objectives

We state the objectives of our proposal for the preservation of the privacy of the borrower.

- **Non-disclosure of social network accounts.** The lending platform should not require the borrower to disclose his accounts. This includes his social network accounts as well as his email accounts. Yet, the borrower should be able to communicate and transact with the lender. Moreover, the lender should be able to compute the social capital score based on the information contained in the social network accounts of the borrower. This information is required by the lender to compute $DISC_x$ and $OPEN_x$. However, he will need to make the computations without learning the information. The borrower should reveal neither the identity of his social network accounts nor their content. Non-disclosure of social network accounts also implies non-disclosure of the biographical identity of the borrower. Otherwise, a simple search on the borrower's name could lead to the discovery of his social network accounts.
- **Non-disclosure of the number of friends.** The borrower will not be required to divulge the precise number of his friends or followers, which is required for the computation of $AUTH_x$.
- **Non-disclosure of personal information.** The borrower will not disclose personal information on the public blockchain or to the lender.

This information, which is required for the computation of HON_x and subsequently SC_x, includes the borrower's name, email address, date of birth, and potentially other personal information. Moreover, as mentioned before, the lender will not have access to the content of the borrower's social network accounts. The lender will also have to compute the variables *bonus*, $CONS$, and SC, without access to the personal information.

- **Disclosure of a subset of friends.** We will tolerate the disclosure of a subset of the friends of the borrower for a given social network account x. We will assume that the subset is indistinguishable enough to not allow the discovery of the identity of the borrower.

6.3 Building Blocks

We describe the building blocks that we use for the preservation of the privacy of the borrower.

- **Homomorphic Cryptosystem.** As stated in [17], let $E_s(.)$ denote the encryption function with the public key PK_s of agent s in an asymmetric cryptosystem C. The cryptosystem C is said to be additive homomorphic if we can compute $E_s(x + y)$, given only $E_s(x)$, $E_s(y)$, and PK_s. For detailed information about homomorphic cryptosystems and their applications, we refer the reader to the thesis [18] of Doerte K. Rappe on this topic.
- **Zero-Knowledge Proof of Set Membership.** As stated in [17], let $F = \{m_1, \ldots, m_p\}$ be a public set of p messages, and $E(m_i)$ be an encryption of m_i with a prover's public key, where m_i is secret. A zero-knowledge proof (ZKP) of set membership allows the prover to convince a verifier that $E(m_i)$ encrypts a message in F.
- **Zero-Knowledge Proof of Plaintext Equality.** As stated in [17], let $E_u(m)$ and $E_v(m)$ be the encryptions of a message m with the public key of agents u and v respectively. A zero-knowledge proof of plaintext equality allows a prover to convince a verifier that $E_u(m)$ and $E_v(m)$ encrypt the same message.
- **Cryptographic Hash Function.** As described in [19] and [20], a cryptographic hash function takes an input of variable size and produces an output of fixed length. For example, for a 256-bit hash function, the output would always be 256 bits in size, if the input is 1 bit, 100 bits, or even 1 gigabits. A cryptographic hash function is efficient to compute. However, for $H(x) = h$, it is computationally infeasible to find x, where $H(x)$ is the function that takes x as input and h is the resulting hash of x. A hash function may be termed as a hiding function or a one-way function due to this property. Additionally, a hash function H is considered to be collision-resistant if it is infeasible to find a pair (x, y), such that $x \neq y$, yet $H(x) = H(y)$. This property allows $H(x) = h$ to be used as a message digest for x. Examples of cryptographic hash functions include SHA-2, SHA-3, and RIPEMD-160.

6.4 Our Proposed Privacy-Preserving Measures

In this section, we discuss our proposed measures that help preserve the privacy of the borrower on our lending platform.

Table 2 summarizes the correspondence between the privacy objectives stated in Section 6.2 and the the privacy-preserving measures that are taken to achieve them.

- **Borrower's pseudonymous identity.** A pseudonym is a fictitious identity of a user that hides his or her true identity. The borrower creates a new unique pseudonymous identity or address on the platform specifically for each new loan request. This identity is considered to have no link to his previous transactions as well as his social network accounts. Creating this identity may be as simple as generating a new public-private key pair. The borrower communicates with the lender using this new identity. Let's denote this pseudonymous identity of the user as b.

  Let's outline how generating a public-private key pair may be used to create a new unique pseudonymous identity for the borrower. This method is described in further detail in the book on Bitcoin and Cryptocurrency Technologies by Narayanan et al. [21]. The method uses a digital signature scheme that has a *generateKeys* operation. This operation generates a public key pk and a corresponding secret key sk. The public key pk is then considered as the

Privacy Objective	Privacy-Preserving Measures
Non-disclosure of social network accounts	• The borrower does not disclose his biographical or his social network identity at any step during the loan request process. • The borrower interacts with the lender only with a new, unique, pseudonymous, and unlinked identity that is created by the borrower on the lending platform.
Non-disclosure of the number of friends	• The borrower and the certifiers publish the value of the exact number of friends only in encrypted form. • The lender is only able to learn a general set that the value belongs to.
Non-disclosure of personal information	• The borrower never reveals any personal information such as email addresses, date of birth, etc. to the lender in cleartext form. • This information is published by the borrower and the certifiers only in encrypted or hashed form.
Disclosure of a subset of friends	• The borrower appoints a subset of his friends as certifiers and discloses this information to the lender. • However, this disclosure does not link the borrower to his social network account as long as the assumption that the subset is indistinguishable enough holds true.

Table 2 Correspondence between the privacy objectives stated in Section 6.2 and the the privacy-preserving measures that are taken to achieve them.

pseudonymous identity of its owner. Any message that originates from the owner of the public key pk needs to be digitally signed by the corresponding secret key sk. All users can verify the authenticity of the message as originating from the owner, since only the true owner knows the corresponding secret key sk and thus only they can emit a correctly signed message. Due to the fact that in practice the public key pk would be a large random and unique number, nobody would be able to associate it with the true identity of the owner. Yet only the owner can use this identity since no other user knows the corresponding secret key.

- **Certifiers.** A borrower b appoints some of his friends from his account on the social network account x as *certifiers*. These are trusted friends who already have access to the borrower's social network content due to their friend status. The certifiers will publish the information gleaned from the borrower's social network account in homomorphic encrypted form. The lender or another verifier will be able to match the information published by the certifiers to the information published by the borrower in order to verify the latter's veracity. In case of inconsistency between the information published by the certifiers, the verifier may choose to believe the information that is certified by a certain majority. The threshold of the majority can be defined by the lender himself, for example, 50%, 75%, or even 100%.
  As stated earlier, we tolerate the disclosure of the identities of the certifiers to the lender. However, the lender does not gain any access to the social network content of the certifiers.
  Please note that the set of certifiers could alternatively be replaced by a single Trusted Third Party (TTP) certifier. This TTP could be the social network operator itself, for example, Facebook, or it could be a certification service provider that has been given access to the social

network account by the borrower. However, this alternative solution would require the existence of such TTPs. In our proposed measures, we do not assume the existence of this third party infrastructure. Moreover, this alternative solution moves the platform towards centralization of trust, which may not be desirable.

- **Verifying the certifiers.** We use a challenge-response authentication protocol to verify the certifiers. In challenge-response authentication protocols, the verifying entity, let's say Alice, presents a challenge to the entity to be verified, let's say Bob. The challenge must be answered by Bob with a correct response that will be checked and validated by Alice. If the response is correct, that is, it satisfies the challenge that was presented, Alice is able to authenticate Bob. The absence of a correct response implies that Bob fails the authentication. The reader may see [22] for further information on challenge-response authentication mechanisms and protocols.
  The lender challenges the certifiers to demonstrate that they are valid account holders on the social network x. The lender sends a different challenge to every certifier on the certifier's presumed account on the social network x. Each challenge comprises of a nonce (number used only once) and the identity of the borrower. A certifier must reply with the unique nonce and a statement such as *"I am indeed a certifier for the borrower b"* from his presumed social network account. The ownership is verified if the identity of the replying account, the nonce, and the statement are correct.
- **How to link the borrower's pseudonymous identity with his social network account?** Let's denote the identity of the borrower b on the social network x as b_x. The borrower publishes the identity b_x in hashed form and links it with his borrower identity b. The information may be published as the tuple $< borrower\_identity, H(social\_network\_account) >$, where $H()$ is the cryptographic hash function. For example, $< b, H(b_x) >$. The borrower then sends the tuple to his certifiers in clear non-hashed form. For example, $< b, b_x >$. The certifiers already know the social network account of the borrower due to their friend status. The certifiers hash the social network account identity on their own and publish the tuple. The hashed data hides the social network account identity of the borrower. However, the hashed data allows comparison of the information published by the borrower and the information published by the certifiers.
  The lender can now verify the equivalence of the information published by the borrower and the certifiers. For example, let's say that a certifier c published $< b, H(b'_x) >$, then the lender can check whether $H(b_x) = H(b'_x)$. Please note that the lender does not learn the social network account identity of the borrower. However, the lender gains confidence through the certifiers that the borrower indeed owns an account on the social network x. Moreover, the borrower's anonymous unique identity b for the loan transaction is permanently linked to his social network account b_x while keeping it anonymous as well.
- **How to disclose the number of friends in a privacy-preserving manner (in order to enable the lender to compute $AUTH_x$ and $DISC_x$)?** The borrower b publishes the number of his friends f in homomorphic encrypted form, that is, $E_b(f)$. The borrower then asks his certifiers to publish the number of his friends in encrypted form as well. The certifiers can retrieve this information independently since they have access to the borrower's social network content. Let's say that a certifier c observes that the number of friends is f'. The certifier then publishes $E_c(f')$.
  After publication of the number of friends in encrypted form by the certifiers, the borrower b and each certifier c jointly generate and publish a plaintext equality zero-knowledge proof to demonstrate the equality of f and f'. The lender will verify the plaintext equality ZKP to gain confidence that both borrower b and certifier c published the same number of friends, that is, $f = f'$, even though the lender does not learn the value.
  Moreover, the borrower b publishes a set membership zero-knowledge proof to demonstrate that the number of friends f belongs to a certain set F_i that is known publicly. These sets can be pre-defined, for example, $F_0 = \{0, 1, \ldots, 99\}$, $F_1 = \{100, 101, \ldots, 999\}$, $F_2 = \{1000, 1001, \ldots, 9999\}$, $F_3 = \{10000, 10001, \ldots, 99999\}$, $F_4 =$

$\{100000, 100001, \ldots, 999999\}$, $F_5 = \{1000000, \ldots\}$, etc. The lender will verify the set membership ZKP to learn the range. Please note that the lender will not learn the precise number of friends. The disclosure of the range places the borrower in a k-anonymous set of other users whose number of friends belong to the same range. In this example, the value of $AUTH_x$ could be calculated as given in Equation 7, where the function $smzkp(E_b(f), F_0)$ returns true if $f \in F_0$.

$$AUTH_x = \begin{cases} 0 & \text{if } smzkp(E_b(f), F_0) = true \\ 0.2 & \text{if } smzkp(E_b(f), F_1) = true \\ 0.4 & \text{if } smzkp(E_b(f), F_2) = true \\ 0.6 & \text{if } smzkp(E_b(f), F_3) = true \\ 0.8 & \text{if } smzkp(E_b(f), F_4) = true \\ 1 & \text{if } smzkp(E_b(f), F_5) = true \end{cases} \quad (7)$$

The above steps enable the lender to compute $AUTH_x$ and $DISC_x$. The lender does not learn the value of the number of friends because it is published in encrypted form by both the borrower and the certifier. However, the lender is still able to verify the validity of the value and learn a general set that the value belongs to. This is possible due to the properties of the homomorphic cryptosystem that is used and the zero-knowledge proofs published by the borrower and the certifier in conjunction with the encrypted values. The homomorphic cryptosystem enables computation on the encrypted values without the need for their decryption.

- **How to publish name, email address, date of birth, etc. in a privacy-preserving manner (in order to enable the lender to compute HON_x)?** The borrower b publishes information such as his name, email address, and date of birth in hashed form along with tags that describe the hidden data. For example, the information may be published as tuples in the format $< data\_tag, H(data\_value) >$, where $H()$ is the cryptographic hash function. Even further information, such as location, interests, groups, etc., may also be published in this manner. Some examples of the published information include: $< name, H(Alice) >$, $< email, H(alice@alice.mail) >$, $< date\_of\_birth, H(01/01/2001) >$, $< location, H(Lyon) >$, $< interest\_01, H(Tennis) >$, $< interest\_02, H(Golf) >$. An agreed upon nonce may be concatenated to a value to be hashed by the borrower and a certifier to further protect the confidentiality of the value. The borrower then sends the published information in clear non-hashed form to his certifiers. The certifiers are assumed to already have access to this information due to their friend status. The certifiers then look up the information on their own on the borrower's social network account; compute the hashes of the information that they find; and then publish the information so that it is visible to the lender in hashed form. The hashed data hides the data values. However, the hashed data allows comparison of the information published by the borrower and the information published by the certifiers.
  The lender can now verify their equivalence. The lender does not need to learn the data values. The lender is interested in whether the borrower is truthful about the information of his social network account. He can achieve this by verifying the equivalence. The lender is able to compute HON_x for each social network account b_x for which the borrower and his certifiers publish the information.

6.5 Security Overview

We first discuss whether the lender is able to compute a correct social score for the borrower on the privacy-preserving platform, despite not being able to learn personal and social network information about the borrower.

The lender is still able to correctly assign a value between 0 and 1 to $AUTH_x$. Instead of using the precise number of friends, which is no longer known, the lender uses the range of friends. For example, $AUTH_x$ could be 0 for the range F_0, 0.1 for the range F_1, and so on. $OPEN_x$ can also still be correctly assigned the value 0 or 1 by the lender. This is because the lender can determine through the certifier verification and the identity linking processes whether the borrower is providing information in encrypted form from his account on the social network x. $DISC_x$ can be derived from $AUTH_x$ and $OPEN_x$ computed above.

Regarding HON_x, as we discussed in the previous section, the lender can correctly assign its

value depending on the extent to which the information published by the borrower and his certifiers matches. This can be done without the need to learn the information itself. The other variables such as SC_x, $bonus$, n, $CONS$, etc. can be either derived from the variables discussed above or calculated in a similar manner.

An underlying assumption for the correctness of the social score is clearly the honesty of the certifiers. The score may be manipulated if the borrower and a majority of the certifiers collude and cheat. However, as we discussed, the lender himself can set the threshold of the majority. For example, the lender could require that at least 75% of the certifiers provide consistent information that validates the information provided by the borrower. Moreover, the lender may also set the threshold for the minimum number of participating certifiers. If these criteria are not met, the lender may consider a borrower as untrustworthy and reject the loan request of the borrower.

We now discuss how effectively the privacy of the borrower is protected in the enhanced privacy-preserving version of our lending platform.

The borrower does not disclose his biographical or his social network identity at any step during the loan request process. The borrower interacts with the lender only with a new, unique, pseudonymous, and unlinked identity that is created by the borrower on the lending platform. The borrower appoints a subset of his friends as certifiers and discloses this information to the lender. However, this disclosure does not link the borrower to his social network account as long as the assumption that the subset is indistinguishable enough holds true.

In the privacy-preserving version of our lending platform, the borrower also never reveals any personal information such as the exact number of friends, email address, date of birth, etc. to the lender in cleartext form. This information is published by the borrower and the certifiers only in encrypted or hashed form. The confidentiality of the information is maintained as long as the security of the cryptosystem and the cryptographic hash function is not breached.

Another obvious assumption for the privacy of the borrower is that none of the certifiers will collude with the lender to reveal his identity and his private information. However, the probability of a certifier acting maliciously is considered low by the borrower since the certifiers are trusted friends who already have access to the borrower's information. Moreover, in case of ambiguity regarding the trustworthiness of a certain certifier, the borrower should be able to ascertain the risk of breach of privacy before appointing them as a certifier.

7 Evaluation

In this section, we evaluate the execution of the social score function on the "Social circles: Facebook" real user dataset. The objective is to determine whether the analysis of real social datasets can help the operator set the parameters of a platform in production.

7.1 Setup of the Test Environment

To evaluate the function itself, we use real user data from the Stanford Network Analysis Project (SNAP). The dataset is called "Social circles: Facebook" [2]. To interpret the dataset and to make calculations based on it, we work with the Anaconda Prompt (docs.anaconda.com) and the python environment Jupyter Notebook (jupyter-notebook.readthedocs.io). Within jupyter notebook, we imported the libraries pandas (pandas.pydata.org) and networkx (networkx.org) as well as matplotlib (matplotlib.org).

7.2 Results and Observations

We used the 107.edges file from the SNAP dataset [2]. It contains 53498 edges (signifying friend relationships) and the corresponding nodes. The dataset is anonymized. As discussed earlier, the number of friends influences the authenticity of a person. Evaluating the data shows that more than a third of all users have more than 50 friends and therefore have a chance to get the best social score if we set the threshold to this value. On the other hand, there are also almost 15% users who do not have more than ten friends and consequently get the worst result in this category. The results are shown in figure 3. In our evaluation, we only differentiate between three steps concerning the number of friends: 10, 30 and 50. Since more than a third of the users have enough Facebook friends to get the best result possible in the "amount of friends" category, we evaluate if a higher limit would be more suitable. For testing

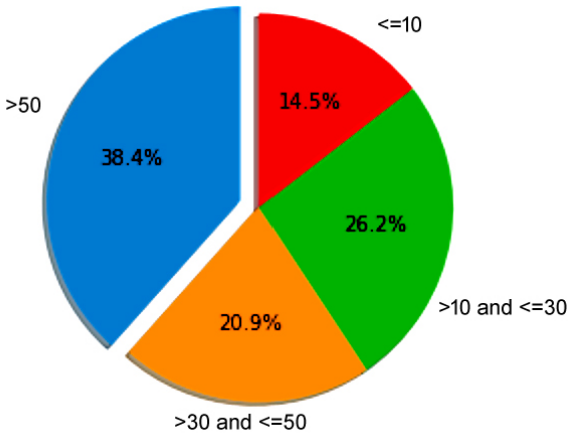

Fig. 3 The biggest part has more than 50 Facebook friends and gets the best result in this category.

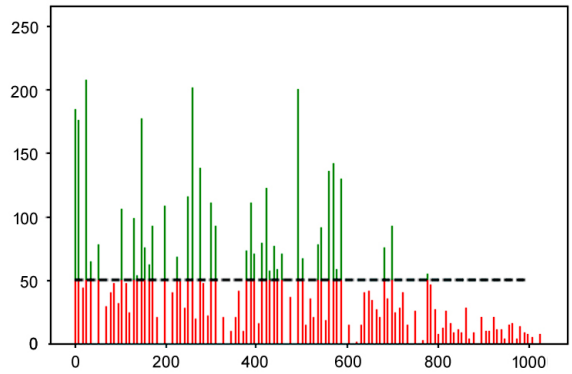

Fig. 4 The x-axis shows the users and the y-axis shows how many Facebook friends each of these users has. 389 out of 1034 users exceed the threshold of 50.

reasons we will adapt these limits. We will start with 200 and then go down to 150, 100 and lastly to 50. The amount of users tested in this experiment is 1034. When we set the threshold to 200, which means that the user needs more than 200 Facebook friends to get the best result in this category, only 12 of the 1034 users qualify for the best result. Subsequently, we obtain the result of 50 users qualified for a threshold of 150, 163 users for a threshold of 100, and finally 389 users for a threshold of 50. The results of this last experiment are plotted in the figure 4. In this experiment, we see that by analyzing real datasets, we can set the thresholds for the platform in order to correspond to the desired rate of users who should qualify. The number of friends is only a small part of the final social score. Other factors include the number of accounts connected, number of pictures posted, account creation date, the bonus for connecting 5 accounts, etc. These factors could not be considered in this experiment due to the absence of this information in the dataset.

8 Conclusion

In this paper, we have presented a new approach to calculate the users' trustworthiness on peer-to-peer lending platforms. This approach is neither collateral nor credit score based. The formula that we use to calculate a user's social score relies on the social capital theory and consequently the information retrieved from the user's social network accounts. It considers how well connected a user is, since connections may help the user achieve professional and personal success. The social score is implemented in a smart contract running on the Ethereum blockchain. The whole lending process is automated and does not need any input from a middleman.

The presented approach offers a new method to verify users' trustworthiness regarding lending, where even users with a non-sufficient credit score and no valuable assets as collateral could get a chance on a loan. We quantified the amount of gas that is consumed by the deployment of the smart contract. Moreover, we also evaluated the execution of the function on a real social network dataset. This experiment demonstrated how we can use analysis of social network data to determine optimal thresholds for a platform in production.

Furthermore, we presented an enhanced version of our lending platform that takes privacy considerations into account. The proposed measures, based on cryptographic building blocks such as zero-knowledge proofs and cryptographic hash functions, enable the platform to preserve the borrower's privacy. We observe that the lender is still able to compute the borrower's social score despite being unable to learn any personal information or even the identity of the borrower.

References

[1] Global Social Media Stats. https://datareportal.com/social-media-users Accessed 2022-03-27

[2] SNAP: Network Datasets: Social Circles: Facebook. https://snap.stanford.edu/data/ego-Facebook.html Accessed 2022-03-27

[3] Zopa: First Peer-to-peer Lending Platform in the UK. https://www.zopa.com/ Accessed 2022-03-27

[4] Businesswire: Global Peer to Peer (P2P) Lending Market Trends, Growth, Opportunity Report 2020-2025. https://www.businesswire.com/news/home/20201215005523/en/\Global-Peer-to-Peer-P2P-Lending-Market\-Trends-Growth-Opportunity-Report\-2020-2025 Accessed 2022-03-27

[5] CoinLoan: Peer-to-peer Lending Platform. https://coinloan.io/ Accessed 2022-03-27

[6] InLock: Peer-to-peer Lending Platform. https://inlock.io/ Accessed 2022-03-27

[7] Prosper: Peer-to-peer Lending Platform. https://www.prosper.com/ Accessed 2022-03-27

[8] Lendingclub. https://www.lendingclub.com/ Accessed 2022-03-27

[9] Fico Score. https://www.fico.com/en/products/fico-score Accessed 2022-03-27

[10] Dubos, R.: Social Capital: Theory and Research, (2017). Routledge

[11] Field, J.: Social capital in policy and practice. In: Social Capital, pp. 84–99 (2016). Routledge

[12] Gurajala, S., White, J.S., Hudson, B., Voter, B.R., Matthews, J.N.: Profile characteristics of fake twitter accounts. Big Data & Society **3**(2), 1–13 (2016)

[13] Ścigała, K.A., Schild, C., Zettler, I.: Dishonesty as a signal of trustworthiness: Honesty-humility and trustworthy dishonesty. Royal Society Open Science **7**(10) (2020)

[14] Hartmann, J., Hasan, O.: A social-capital based approach to blockchain-enabled peer-to-peer lending. In: The Third IEEE International Conference on Blockchain Computing and Applications (BCCA 2021), pp. 105–110 (2021)

[15] Hayes, G.: The Beginners Guide to Using an Ethereum Test Network. https://medium.com/compound-finance\/the-beginners-guide\-to-using-an-ethereum-test-network\-95bbbc85fc1d Accessed 2022-09-10

[16] IBM: What Are Smart Contracts on Blockchain? https://www.ibm.com/topics/smart-contracts Accessed 2022-09-10

[17] Hasan, O., Brunie, L., Bertino, E., Shang, N.: A decentralized privacy preserving reputation protocol for the malicious adversarial model. IEEE Transactions on Information Forensics and Security **8**(6), 949–962 (2013)

[18] Rappe, D.K.: Homomorphic Cryptosystems and their Applications. Cryptology ePrint Archive, Paper 2006/001. https://eprint.iacr.org/2006/001 (2006). https://eprint.iacr.org/2006/001

[19] Cryptographic Hash Functions. https://www.ics.uci.edu/{\texttildelow}keldefra/teaching/fall2016/uci_compsci134/slides/LEC5-KED.pdf Accessed 2022-03-27

[20] Cryptography Hash Functions. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm Accessed 2022-03-27

[21] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: a Comprehensive Introduction. Princeton University Press, Princeton, NJ, United States (2016)

[22] Challenge Response Authentication Mechanism (CRAM). https://www.geeksforgeeks.org/challenge-response-authentication\-mechanism-cram/ Accessed 2022-09-10