May 2023

QUANTIFY PEER-TO-PEER (P2P) PAYMENT TRUST

JUSTIN MARCIANO
VISA

“QUANTIFY PEER-TO-PEER (P2P) PAYMENT TRUST”

VISA

INVENTORS:

JUSTIN MARCIANO

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to Peer-to-Peer (P2P) payment methods, and particularly to a method and system for quantifying P2P payment trust.

BACKGROUND

[0002] Peer-to-peer payment (P2P) methods allow performing transactions between individuals who trust each other. However, P2P payment methods currently have very few security solutions. According to research, 13% of people who have used various P2P payment applications such as PayPal®, Venmo™, Zelle® or CashApp™ say they have sent someone money and later realized it was a scam. Additionally, amid a jump in popularity of P2P payment methods, security and fraud concerns put P2P users at risk of losing money. Nearly a quarter (~23%) of P2P users have sent money to the wrong person, and 15% have been victims of scams. For those who use P2P services several times a week, these percentages jump to 42% and 22%, respectively. The additional issue with the errors/scams in the P2P payment methods is that the liability falls on the user initiating the payment, given the existing regulations do not protect against fraud in instances where individuals are tricked into authorizing payments themselves.

[0003] In other words, the P2P payment methods rely on trust, sacrificing user security for the sake of convenience. The use and popularity of P2P payment methods will only increase with time, as the payment market was $1.8T in 2021 and is expected to surpass $5.2T by 2028. Inevitably, fraud numbers will increase over time due to more sophisticated fraud methods that will likely target payment application with refund difficulty or flaws in refund policies. Thus, the true way to protect users is to make them aware of their surroundings or other users, without inappropriately exposing users' data.

[0004] Thus, there exists a need to address the above limitations and provide a secure way of providing P2P payment methods with enhanced user experience, incentivize active use of the application, and decrease fraud levels.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the

figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0006] **Figs. 1a-1b** illustrate exemplary architecture that implements embodiments consistent with the present disclosure.

[0007] **Fig. 2** shows a flow diagram illustrating a method for performing an efficient P2P payment according to embodiments consistent with the present disclosure.

[0008] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0009] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0010] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0011] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0012] The terms “comprises,” “comprising,” or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0013] The terms "an embodiment," "embodiment," "embodiments," "the embodiment," "the embodiments," "one or more embodiments," "some embodiments," and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0014] The terms "including," "comprising," “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0015] **Figs. 1a-1b** illustrate exemplary architectures that implement embodiments consistent with the present disclosure. In an embodiment, when it comes to P2P payment, there is an incredible amount of trust that is needed between two parties as these transactions are from one individual to another. Therefore, most people only use these applications with people they are comfortable with, but this is slowly changing. With the rapid. growth of P2P payment applications, people are starting to venture into the unknown more casually and frequently, and end up sacrificing security because the P2P methods are easy and convenient to use.

[0016] The present disclosure enables a P2P payment application interface to access data required to calculate a social accountability metric for a user. The social accountability metric may comprise a trust score indicative of good payment behavior or bad payment behavior of users using P2P applications. Depending on the trust score calculated, a trust level will be assigned to users as “Very Low,” “Low,” “Medium,” “High,” or “Very High”. The trust score incentivizes the users to use the P2P applications more frequently and encourages good payment behavior while allowing users to make their own decisions while initiating a payment. A detailed explanation of Figs.1a-1b is provided below.

[0017] In one implementation, the exemplary architecture **100a** for providing an efficient peer-to-peer (P2P) payment system is shown in Fig. **1a**. The exemplary architecture **100a** includes a system **101** comprising an Application Programming Interface (API) **103** and a memory **105**. In some embodiments, the system may include a payment server or a Visa server. The system **101** may be configured to receive or collect data related to a plurality of variables corresponding to a user's P2P payment account. In some embodiments, the data may be received from various sources. As an example, the sources may include, but not limiting to, one or more P2P applications like PayPal®, Venmo™, Zelle® or CashApp™, which are currently being used by the user. The system **101** may be configured to calculate a trust score for an account associated with different users based on the received data. The API **103** may be configured to calculate the trust score for a plurality of variables, using which a final trust score is computed for the user.

[0018] In an embodiment, the system **101** may include, but not limited to, a microprocessor, a processor, central processing unit, digital signal processing unit, single core processor, dual core processor, quad core processor, mobile device processor, desktop processor, a System-on-Chip (SoC) device, Complex Instruction Set Computing (CISC) microprocessor, a reduced instruction set computing (RISC) microprocessor, a Very Long Instruction Word (VLIW) microprocessor, or any other type of processor or processing circuit on a single chip or integrated circuit.

[0019] In some embodiments, the API **103** may be interfaced to the memory **105** configured to store the sub-scores or score for the account of users. The memory **105** may include a computer storage media which may include a Random Access Memory (RAM), a Read Only Memory (ROM), a flash memory or other solid state memory units, a Complete Disc-Read Only Memory (CD-ROM), a Digital Versatile Disks ("DVD"), or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information, and which can be accessed by a computer, mobile phone, laptop, tablet etc.

[0020] Further, the system **101** may be communicably coupled to a user device **107,** which is used by the user to carry out a P2P transaction. In some embodiments, the system **101** may be coupled to the user device **107** via a communication network (not shown). In some embodiments, user device **107** may include but not limited to, a computer, a laptop, a tablet, a

PC, a mobile phone etc. The user device **107** may comprise a display **109** configured to display trust level of P2P payment app account of different users.

[0021] The explanation of Fig. 1a is provided in conjunction with Fig. 1b, which is an exemplary scenario to understand the invention with ease. In an embodiment, the API **103** may be configured to receive data for a plurality of variables (i.e., collecting data for each variable, as shown in step 1 of Fig. 1b. The plurality of variables may comprise, but not limited to, an age of user's P2P payment account, total payment value, number of outstanding payments, sum of outstanding payments, number of payment methods on platform, number of payment method declined, average time of payment completion, business account status, international transfers, average amount sent/received, payment frequency, bad actor behavior and the like. As an example, the data received for the variable "age of account" may include information such as from how long the account of the user is active. The data received for the variable 'total payment volume' may include information such as how many transactions or payments have been performed from the user's account. Once the data of each variable is received, the API **103** may be configured to calculate a trust score for each variable of the plurality of variables based on a predefined algorithm, for example, or using Visa score algorithm as shown in step 2 of Fig. 1b, where the variables are fed into the Visa score algorithm. In an embodiment, the API **103** may calculate a sub-score between "-0.5" and "0.5" for each variable.

[0022] For example, the sub-score for each of the variable may be calculated in the below manner:

A. **Age of account variable:** for each year the account has been active, the sub-score is added with 0.05 up to a maximum of 0.5.

B. **Total payment volume variable:** divide the total payment volume by the average payment volume for all users, then subtract 0.5 from the result to get the sub-score.

C. **Number of outstanding payments:** divide the number of outstanding payments by the average number of outstanding payments for all users, then subtract 0.5 from the result to get the sub-score.

D. **Sum of outstanding payments:** divide the sum of outstanding payments by the average sum of outstanding payments for all users, then subtract 0.5 from the result to get the sub-score.

E. **Number of payment method on platform:** for each payment method on the platform, add 0.1 to the sub-score, up to a maximum of 0.5.

F. **Number of payment method declined:** divide the number of payment method declined by the average number of declined for all users, then subtract 0.5 from the result to get the sub-score.

G. **Average time of payment completion:** calculate the difference between the average time of payment completion for the user and the overall average time for all users, then divide by the overall average time and subtract 0.5 from the result to get the sub-score.

H. **Business account status:** if the account is a verified business account, add 0.5 to the sub-score. If it is not, do not adjust the sub-score.

I. **International transfers:** if the account has made international transfers, add 0.2 to the sub-score. If it has not, do not adjust the sub-score.

J. **Average amount sent/received:** divide the average amount sent/received by the overall average for all users, then subtract 0.5 from the result to get the sub-score. If the average amount sent/received is more than $50, add 0.2 to the sub-score.

K. **Payment frequency:** calculate the difference between the average payment frequency for the user and the overall average frequency for all users, then divide by the overall average frequency and subtract 0.5 from the result to get the sub-score.

L. **Bad actor behavior:**

If the account has been flagged for fraud, scam, or money laundering, subtract 0.5 from the sub-score.

If the account has not been flagged for any bad actor behavior, do not adjust the sub-score.

[0023] In an embodiment, subsequent to calculating the sub-scores for each of the variables, the API **103** may sum up all the sub-scores to get the overall trust score for the user's account. In an embodiment, the API **103** may be configured to assign a trust level based on the calculated trust score (i.e., step 3 of Fig. 1b, where the quantifiable trust score is calculated/assigned). As an example, a correlation between the trust score and the overall trust level assigned to the users is summarized below:

a. if the overall trust score is less than 0, then the API **103** may assign a trust level of "Very Low".

b. If the overall trust score is between 0 and 0.2, a trust level is assigned as "Low".

c. If the overall trust score is between 0.2 and 0.4, the trust level is assigned as "Medium".

d. If the overall trust score is between 0.4 and 0.6, the trust level is assigned as "High".

e. If the overall trust score is greater than 0.6, the trust level is assigned as “Very High”.

[0024] As shown in step 4 of Fig. 1b, the trust score is sent to the P2P app. Next, the API **103** may be configured to display the trust level for the user’s account on a user’s device or P2P payment application profile of the user (i.e., step 5 score is displayed as trust level on the P2P app profile of the user). As an example, the trust level may be displayed as “High” or “Very High” on the P2P app profile, indicating a good payment behavior of the account user. Whereas a trust level of “Low” or “Very Low” may indicate a bad payment behavior of the account user. Having a bad score may be embarrassing for the account user and incentivize the user to be “better” at using the P2P payment methods.

[0025] In a non-limiting example, user A may wish to initiate payment for some purchase via a P2P payment application installed on his/her mobile device. Suppose user A is not aware of the identity of the other user receiving the payment and the other user is scamster. In such scenarios, while performing the transaction, user A may get trapped for performing an unauthorized transaction or may fall into a scam/fraud, where the user A may lose his money from the account. In such cases, the scamsters or fraudulent users have been taking advantage of the virtual nature of the P2P payment platform and the restrictions it has on repayment or reversing an already completed transaction. In this scenario, user A may be demotivated to use such P2P payment methods as he/she may not get the refund for the unauthorized transactions. This problem is solved by the present disclosure, which will help user A to identify the genuineness, accountability, and trustworthiness of the account to which the payment is being made. The trust score and the trust level of the receiving user, which is displayed on the user’s P2P application, may be helpful for deciding whether the user is transacting with a genuine/trustworthy user, and thereby improving security against fraudsters and scammers The trust score and the trust level are a reliable means for verifying the authenticity or trustworthiness of the users, since the trust score is calculated from impersonal, unrevealing, and unbiased data of the users. Accordingly, the trust level and the trust score incentivize the users to use the P2P payment methods more frequently and encourage good payment behavior while allowing users to make their own decisions.

[0026] **Fig. 2** shows a flow diagram illustrating a method **200** for providing a secure peer-to-peer payment according to embodiments consistent with the present disclosure.

[0027] As illustrated in Fig. **2**, the method of providing a secure Peer-To-Peer payment (P2P) application. The method may include interaction between a P2P Application Programming Interface (API) **103** and a user device **107**.

[0028] In an embodiment, the method at step **201** may comprise receiving data for each variable of a plurality of variables from a plurality of sources. As discussed earlier, the plurality of sources may include but not limited to P2P applications/platforms.

[0029] As shown in step **203**, the method may comprise calculating a trust score based on the received data for each of the variables. The trust score may be calculated by computing sub-score of each variable and determining the average or sum of the overall sub-scores.

[0030] Further, the method may comprise assigning a trust level based on the calculated score as shown in step **205**. The trust level may be assigned as "Low," "Very Low," "High," "Medium," or "Very High" for the P2P payment app of the associated user.

[0031] At step **207**, the method may comprise displaying the trust level on a display **109** of P2P payment app profile of the user. This score and trust level incentivize users to use P2P apps more frequently and encourages good payment behavior while allowing people to make their own decisions.

[0032] In an embodiment, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. A non-transitory computer readable medium may include media such as magnetic storage medium, optical storage, volatile and non-volatile memory devices etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0033] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries.

[0034] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building steps have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0035] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

"QUANTIFY PEER-TO-PEER (P2P) PAYMENT TRUST"

ABSTRACT

The present disclosure provides a method and system which enables P2P payment application interfaces to access data required to calculate a social accountability metric comprising a trust score indicative of good payment behavior or bad payment behavior of users using the P2P applications. Depending on the score calculated, the trust level will be assigned as "Very Low," "Low," "Medium," "High," or "Very High" for the P2P payment account of the users. This score incentivizes users to use the P2P apps more frequently and encourages good payment behavior while allowing people to make their own decisions.

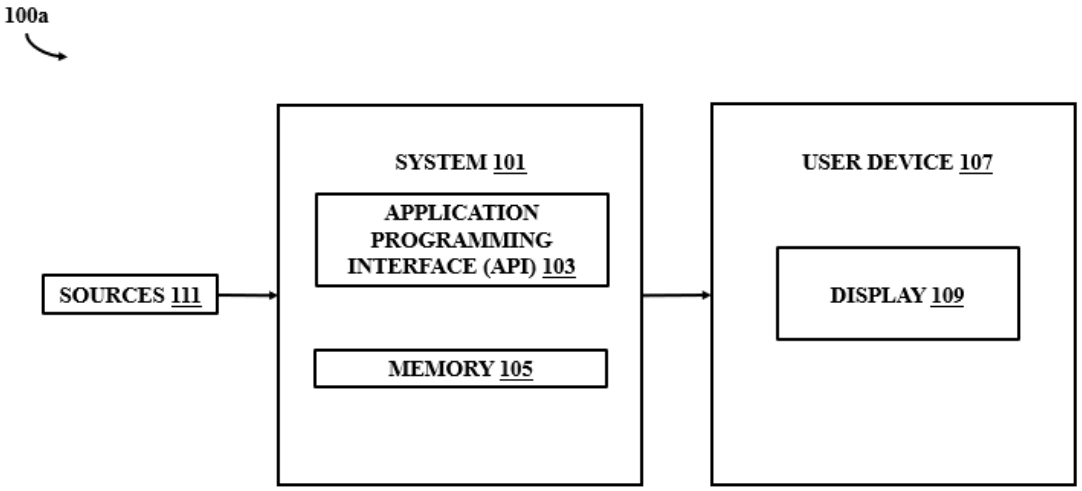
100a
SYSTEM 101
APPLICATION PROGRAMMING INTERFACE (API) 103
MEMORY 105
SOURCES 111
USER DEVICE 107
DISPLAY 109

Fig. 1a

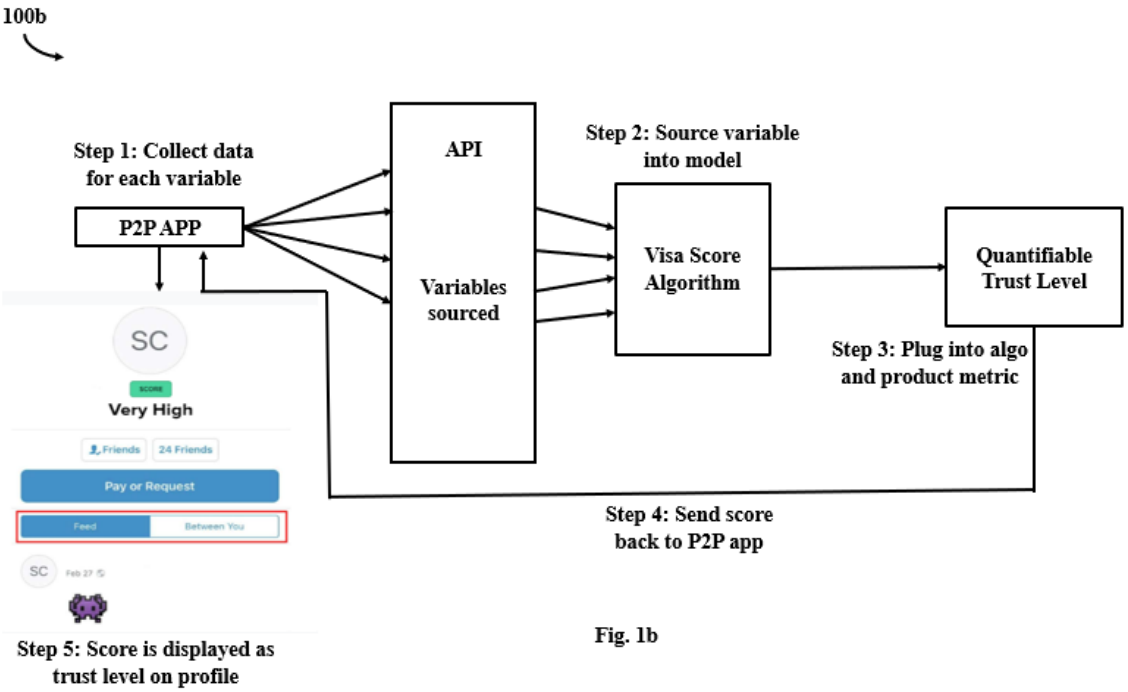
100b
Step 1: Collect data for each variable
P2P APP
API
Variables sourced
Step 2: Source variable into model
Visa Score Algorithm
Quantifiable Trust Level
Step 3: Plug into algo and product metric
Step 4: Send score back to P2P app
SC
Very High
Pay or Request
Step 5: Score is displayed as trust level on profile

Fig. 1b

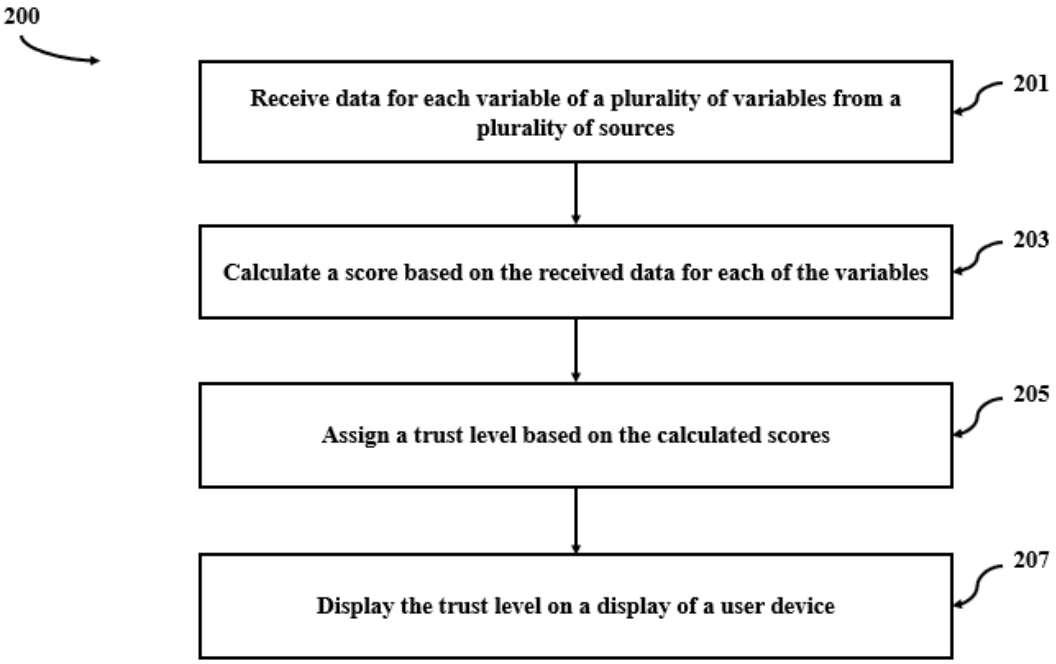
200
Receive data for each variable of a plurality of variables from a plurality of sources
201
Calculate a score based on the received data for each of the variables
203
Assign a trust level based on the calculated scores
205
Display the trust level on a display of a user device
207

Fig. 2