Technical Disclosure Commons

Defensive Publications Series

December 2022

SECURE AND TRUSTWORTHY SYSTEM AND METHOD OF PROVIDING CHARITABLE CONTRIBUTIONS USING CRYPTOCURRENCIES

ILA MALDE
VISA

DEVINA ARVIND
VISA

RAJ PATEL
VISA

AKSHAT AGARWAL
VISA

MANASA BALAJI
VISA

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
MALDE, ILA; ARVIND, DEVINA; PATEL, RAJ; AGARWAL, AKSHAT; and BALAJI, MANASA, "SECURE AND TRUSTWORTHY SYSTEM AND METHOD OF PROVIDING CHARITABLE CONTRIBUTIONS USING CRYPTOCURRENCIES", Technical Disclosure Commons, (December 12, 2022)
https://www.tdcommons.org/dpubs_series/5552

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

“SECURE AND TRUSTWORTHY SYSTEM AND METHOD OF PROVIDING CHARITABLE CONTRIBUTIONS USING CRYPTOCURRENCIES”

VISA

INVENTORS:

ILA MALDE

DEVINA ARVIND

RAJ PATEL

AKSHAT AGARWAL

MANASA BALAJI

TECHNICAL FIELD

[0001] The present disclosure relates to the field of cryptocurrency transactions. Particularly, the present disclosure relates to a secure and trustworthy system and method of providing charitable contributions using cryptocurrencies.

BACKGROUND

[0002] Poverty exists everywhere in the world. To help the needy and poor people, in the existing society there are many philanthropic entities which focus on specific social causes and serve public at large. The philanthropic entities may help the needy people by providing charity in various forms such as money, food, clothing and the like. Also, the philanthropic entities may receive donations from donors. Donors are the end users who donate the funds to needy people. However, since the donations often pass-through middlemen (e.g., non-profit organizations) before they are received by the end recipients, it is necessary to monitor whether the donations reached the end recipients. Donors do not have any visibility with respect to who receives the payment and how donations are used by the recipients, thus leading to lack of transparency. Also, currently, not all non-profit organizations or the philanthropic entities are trustworthy, and there is possibility of fraud involved in the name of non-profit organizations. Thus, the donors are often not sure if the charitable organizations that they are interacting with are credible or fraudulent. Thus, there is a need for a more secure and trustworthy system and method for providing charitable contributions by the donors.

SUMMARY

[0003] Present disclosure relates to secure and trustworthy system and method of providing charitable contributions using cryptocurrencies. Initially, a registration request may be received from a donor. The request may be received by a node in a private consortium blockchain network. Also, a registration request from a recipient may be received by a node in the private blockchain network. The registration request may include sensitive information of the recipient which is verified by one or more members operating in the private blockchain network as being a legitimate recipient of a charitable donation for a cause. Further, the node of the blockchain network may write a recipient identifier with the cause to the private blockchain network. The node of the

blockchain network may receive a request to donate an amount of cryptocurrency from the donor to the recipient. Finally, the node of the blockchain network facilitates a transfer of an amount of cryptocurrency from the donor to the recipient, which uses a public cryptocurrency blockchain.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0005] **FIG.1** shows a secure and trustworthy system for providing charitable contributions using cryptocurrencies, in accordance with some embodiments of the present disclosure.

[0006] **FIG.2** shows an exemplary scenario of a federated blockchain model to validate the transactions performed during the charitable contribution, in accordance with some embodiments of the present disclosure.

[0007] **FIG.3** shows a flow diagram that illustrates a sign-up process for the donor to provide a charity to the recipient, in accordance with some embodiments of the present disclosure.

[0008] **FIG.4** shows a flow diagram that illustrates a sign-up process for the recipients to receive the charity provided by the donors, in accordance with some embodiments of the present disclosure.

[0009] **FIG.5** shows a flow diagram that illustrates an additional sign-up process for the recipients to receive the charities provided by the donors, in accordance with some embodiments of the present disclosure.

[0010] **FIG.6** shows a flow diagram that illustrates the donor searching for a particular cause to provide charity to recipients, in accordance with some embodiments of the present disclosure.

[0011] **FIG.7** shows a flow diagram that illustrates the process of learning the tutorials in an application, in accordance with some embodiments of the present disclosure.

[0012] **FIG.8** shows a block diagram for tax report, in accordance with some embodiments of the present disclosure.

[0013] **FIG.9** shows a block diagram that illustrates donor searching for a particular cause to provide charity to recipients, in accordance with some embodiments of the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0019] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the invention as it is oriented in the drawing figures. However, it is to be understood that the invention 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 embodiments or aspects of the invention. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0020] As used herein, the term “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments. A user can be a sender or a receiver.

[0021] As used herein, the term “user device” can be a computing device operated by a user. A user device can be a sender device or a receiver device. Examples of user devices may include a mobile phone, a smart phone, a personal digital assistant (PDA), a laptop computer, a desktop computer, a server computer, a vehicle such as an automobile, a light client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user input. The user device may also include one or more input sensors for receiving user input. The user device may comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G, or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network.

[0022] As used herein, the term “public/private key pair” may include a pair of linked cryptographic keys. A public key may be used for functions such as encrypting a message to send to an entity that holds the private key, or for verifying a digital signature which was supposedly

made by the entity. The private key may be used for functions such as decrypting a received message or applying a digital signature. Public and private keys may be in any suitable format, including those based on RSA or elliptic curve cryptography (ECC).

[0023] As used herein, the term “blockchain network” may be any set of nodes (computer systems and components) configured to provide verification for interactions. A blockchain network may comprise a distributed computing environment utilizing several nodes that are interconnected via communication links, using one or more computer networks or direct connections. A blockchain network may be implemented over any appropriate network, including an intranet, the Internet, a cellular network, a local area network or any other such network or combination thereof. Components used for such a system can depend at least in part upon the type of network and/or environment selected. Protocols and components for communicating via such a network are well known and will not be discussed herein in detail. Communication over the blockchain network can be enabled by wired or wireless connections and combinations thereof. Nodes may be independently operated by third parties and may be added to, or removed from, the blockchain network on a continuous basis. In some embodiments, a node in a blockchain network may be a full node.

[0024] As used herein, the term “node” can be a “computer node,” which can be any computer or device that connects to the blockchain network. A node that can fully verify each block and interaction in a blockchain can be a full node. A “full node” can store the full blockchain (i.e., each block and each interaction). A “client device” may be a computer node in the blockchain network. A client device can store less than the full blockchain.

[0025] As used herein, the term "blockchain" can be a distributed database that maintains a continuously-growing list of records secured from tampering and revision. A blockchain may include a number of blocks of interaction records. Each block in the blockchain can contain also include a timestamp and a link to a previous block. Stated differently, interaction records in a blockchain may be stored as a series of "blocks," or permanent files that include a record of a number of interactions occurring over a given period of time. Blocks may be appended to a blockchain by an appropriate node after it completes the block and the block is validated. Each

block can be associated with a block header. In embodiments, a blockchain may be distributed, and a copy of the blockchain may be maintained at each full node in a verification network. Any node within the verification network may subsequently use the blockchain to verify interactions.

[0026] As used herein, the term “block header” can be a header including information regarding a block. A block header can be used to identify a particular block an a blockchain. A block header can comprise any suitable information, such as a previous hash, a Merkle root, a timestamp, a nonce, and a Merkle tree root. In some embodiments, a block header can also include a difficulty value.

[0027] As used herein, the term “address” can be a string of characters that identifies a destination or particular location in a data storage system. Values can be provided to a user at a particular address. A sender can send a value to a receiver address of a receiver. An address can be a numerical value that is equivalent to or derived from a public key. For example, a receiver address can be a receiver public key or derived from the receiver public key.

[0028] As used herein, the term “interaction” can include a reciprocal action or influence. An interaction can include a communication, contact, or exchange between parties, devices, and/or entities. Example interactions include a transaction between two parties and a data exchange between two devices. Interactions can also be agreements, contracts, and the like.

[0029] As used herein, the term “verification” and its derivatives may include a process that utilizes information to determine whether an underlying subject is valid under a given set of circumstances. Verification may include any comparison of information to ensure some data or information is correct, valid, accurate, legitimate, and/or in good standing.

[0030] As used herein, the term “processor” may include a device that processes something. In some embodiments, a processor can include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or

Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0031] As used herein, the term “memory” may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0032] As used herein, the term “server computer” may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0033] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0034] Some non-limiting embodiments or aspects are described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0035] **FIG.1** shows a secure and trustworthy system for providing charitable contributions using cryptocurrencies, in accordance with some embodiments of the present disclosure shows.

[0036] In FIG.1, a schematic diagram of a system **100** includes a donor **102**, a browser **104**, and a recipient family **106**. Initially, a user may perform a transaction using the user device **101**. Initially, the donor **102** may use a browser **104** to make donations to recipient family **106**. The browser **104** may further include front end **108** and backend **110**, where the backend **110** may include private consortium blockchain **112** and a public blockchain **114**. The donors **102** may be end users who may be willing to donate funds or charity to the recipient family **106**. The recipient family **106** may be one or more end-users who receives the charity or funds provided by the donor **102** through the browser **104.** Further, the donor **102** and the recipient family **106** may directly interact with each other using the front end **108** of the browser **104**. Whereas, at the backend **110** the donors **102** and the recipient family **106** may be authenticated to determine whether the donors **102** and the recipient family **106** are legitimate or not legitimate. Particularly, the private consortium blockchain **112** may be a group of two or more organizations who are connected in a network as shown in **FIG. 2**. Smart contracts for the Giving Indigent the Funds to Thrive (eGIFT) application will be deployed on a private consortium blockchain **112**. The users of the private consortium blockchain **112** may comprise a diverse range of organizations (e.g., government agencies, financial institutions, non-profit organizations, philanthropists, and etc.). Smart contracts on the blockchain may enforce rules relating to the storage of sensitive recipient data (e.g., Social Security Number, PAN, etc.), assessing of the recipient's family **106**, and processing of the cryptocurrency transactions. The consortium blockchain **112** (i.e., private blockchain) may integrate with a public blockchain **114** (e.g., a Bitcoin blockchain or Ethereum blockchain). The public blockchain **114** may store and facilitate transactions for the peer-to-peer donations between the donors **102** and the recipient family **106**. The data in the public blockchain **114** will be accessible to all users of the eGIFT application.

[0037] In the present disclosure, initially the donor **102** and the recipient family **106** may sign-up with a donation service using the browser **104** before the donation happening between the donor **102** and recipient family **106**, particularly using an eGIFT application installed in user device associated with the donor **102** and the recipient family **106**. The donor **102** may sign-up as "Donor" and the recipient family **106** may sign-up as "Recipient". The sign-up process of the donor **102** is as shown in **FIG.3**. In FIG.3, the donor **102** may either create a cryptowallet or link cryptowallet. The donor **102** may create a cryptowallet and may check balance of by account or by currency or by rewards. Also, the donor **102** may create or link to a sender cryptocurrency wallet to send

donations, and the recipient family **106** may create or link to a recipient cryptocurrency wallet to receive donations. The donor **102** may perform donations using uniswap to exchange or may directly transfer to bank account. Once the donor **102** has signed-up. Similarly, the recipient family **106** may also has to sign-up and create a wallet for receiving donations provided by donors **102**.

[0038] The recipient family **106**, upon signing up to the browser **104**, may log in to a host site that operates the donation service using the browser **104**. Once the recipient family **106** logs in, the recipient family **106** may register for a cause among the list of causes to receive donations from donors **102** as shown in **FIG.4**. For example, the one or more causes may be but not limited to disaster relief, disability, low income, education and senior citizens. Among the list of causes, the recipient family **106** may select an appropriate cause that fits their situation and enter the amount of donation they are seeking. The recipient family **106** may also provide information about their cause and also information showing that their cause is legitimate. The information may include a description of their cause or situation, proof that the consortium approved of their registration with the system, etc. Also, the recipient family **106** may not be visible to the donors **102** unless their registration is successful, since the public blockchain **114** only stores the registered recipients family **106**.

[0039] In some embodiments, the recipient family **106** request to provide an authorization ID by the private consortium blockchain **112**. Further, one or more members of the private consortium blockchain **112** may assess whether the recipient family **106** is legitimate and authentic. If the assessment is successful, then recipient family **106** is registered successfully and is provided the authorization ID. The authorization ID may be proof that the consortium operating the private consortium blockchain **112** approved the registration of the recipient family **106**. Upon the successful registration the recipient family **106** may be added to the registered recipient list under the specified cause along with the approved amount of donations that they are willing to seek. For example, the one or more causes may include bit not limited to natural disaster, education, health issues and the like. Also, the recipient family **106** information that was submitted during the registration and assessment may be stored in the private consortium blockchain **112**.

[0040] However, if the assessment of the recipient family **106** is unsuccessful, one or more members of the private consortium blockchain **112** may request for additional information so that

recipient family **106** is further assessed. The additional assessment of the recipient family **106** is as shown in **FIG. 5**. The recipient family **106** may provide additional information to receive and authorization ID and may get register for the cause to the member of the private consortium blockchain **112** after failing the first attempt of registration. For example, the additional information may include, but not limited to the identification details of the recipient family **106** such as social security number, tax filing household income, date of birth, contact information, insurance information and other documents supporting evidence. Further, the members of the private consortium blockchain **112** may assess the recipient family **106** for the second time with additional information. Upon the successful assessment, the recipient family **106** may be added to the registered recipient list under the specified cause along with the approved amount of donations that they are willing to seek. Also, the additional information provided by the recipient family **106** during the registration and assessment may be stored in the private consortium blockchain **112**.

[0041] For example, consider a scenario where the recipient family **106** may need donations for the cause being natural disaster. In such cases, the recipient family **106** may register under the cause "natural disaster" in the eGIFT application installed on a user device **105**. Further, the recipient family **106** may provide details such as the amount of donations they are willing to receive and also send a request to provide an authorization ID. The request may be sent to a non-profit organization who is a member of the private consortium blockchain **112**. The recipient family **106** may provide the non-profit organizations with information that proves that their house was flooded by showing them pictures, address, social security number, and etc. Upon reviewing the case, the non-profit organization may register the recipient family **106** to the registered recipient list under the cause "natural disaster" and give the authorization ID. Additionally, the information provided by the recipient family **106** may get stored in the private consortium blockchain **112**.

[0042] However, if the non-profit organization rejects the request, and asks the recipient family **106** to provide more evidence, the recipient family **106** may further provide additional information such as contact information, insurance information, tax filing household income, etc., to the non-profit organization. The non-profit organization, in order to verify the additional information, may bring other members of the consortium such as government agencies to verify the additional information of the recipient family **106**. After reviewing the additional information, the non-profit

organization may accept the request and add the recipient family **106** to the registered recipient list under the cause "natural disaster" and give the authorization ID. The information provided by the recipient family **106**, including the additional information, may get stored in the private consortium blockchain **112**.

[0043] The members of the private consortium blockchain **112** as shown in FIG. 2 can build a near real-time system designed to connect various entities using matching algorithms and biometrics to ensure that the rightful recipients family **106** get their intended donations. The expected outcome of building such system is to raise social return on investment (SROI) through increased adoption. The members of the private consortium blockchain **112** include financial institutions, government service departments, merchants, payment network organizations, and etc.

[0044] In some embodiments, the financial institutions may host a thrift card program for the underserved, underbanked to encourage them to open an account in their bank. Financial institutions may also increase access to financial education and services to these account holders and their family members. The government service departments may support the thrift card program to incentive the claimants to participate and allow their money to be sent directly to the account. The merchants may leverage their value-added service program through a payment network organization to issue surplus goods to the thrift card holders. The payment network organization has various programs, whose Application Programming Interfaces (APIs) can be leveraged for the consortium group to give back to the registered underserved.

[0045] In some embodiments, the payment network organization may build artificial intelligence models to help the disadvantaged by matching the registered "donors" to the registered "recipients" using blockchain technologies to ensure the cryptocurrencies are deposited directly to end users.

[0046] Upon the successful registration of the donor **102** and the recipient family **106**, the donor **102** may log in to the browser **104** to provide the donations to the recipient family **106** as shown in **FIG.6**. Once donor **102** logs in, a list of choices are displayed to the donor **102**. For example, the list of choices is illustrated in a display **105**, wherein the donor **102** is displayed with CryptoBytes, Search for Cause, Donate One-Time, Donate Recurring, My contribution history, and Access Wallet. Further, donor **102** can select "Search for Cause" to search for different causes that the donor **102** can donate to. Upon selecting the option "Search for Cause," donor **102** may be presented with different causes and the donor **102** may select one or more of the causes to donate

to. For example, the one or more causes may be “disaster relief”, “disability”, “low income”, “education”, “senior citizen”, and the like. Upon selecting a cause, donor **102** may be displayed with a registered recipient list under the specified cause that the donor **102** selected. Each registered recipient family **106** in the registered recipient list displays only cryptocurrency wallet address, the amount of donations already received, and the target amount of donations. Donor **102** may select a recipient family **106** among the registered recipient list and send donations to the recipient family **106**.

[0047] For example, consider a scenario where the donor **102** wishes to donate to a recipient family **106** who was impacted by a natural disaster. The donor **102** may launch the eGIFT application and log in to the eGIFT application and select “Search for Cause”. Upon selecting “Search for Cause”, the donor **102** will be presented with different causes such as “natural disaster”, “disability,” etc. When the donor **102** selects the “natural disaster”, the donor **102** is also presented with a registered recipient list under the “natural disaster” of (111111, 2/10), (222222, 0/10), and (333333, 1/20), where the first number is the cryptocurrency wallet address, and the second number stands for the amount of cryptocurrency received relative to the target amount of cryptocurrency. The donor **102** may choose the recipient family **106** with the cryptocurrency wallet address “111111” and send 1 cryptocurrency donation. Once the transaction is processed, the recipient will have updated the amount of “3/10” cryptocurrency.

[0048] The transactions of donations between the donor **102** and the recipient family **106** are stored and facilitated in the public blockchain **114**. The public blockchain **114** can have smart contracts (e.g., as in Ethereum). The smart contracts on the public blockchain **114** can include limits regarding how much cryptocurrency donation can be made in one transaction, the recipients family **106** for specific causes, etc.

[0049] The consortium members of the private consortium blockchain **112** can assess the recipient family **106**. The recipient family **106** may provide data that proves their cause is legitimate and the members of the consortium blockchain **112** can review the data. If the recipient’s family **106** is approved, they are added to a registered recipient list of the public blockchain **114**, while the private consortium blockchain **112** stores the data of the approved recipient family **106**.

[0050] The registered recipient list of the public blockchain **114** can be divided by different causes. To protect the identities of the registered recipient family **106**, the registered recipients list stores

only causes, cryptocurrency wallet addresses, the amount of donations, and the amount of donations received of the registered recipient family **106**. Since the public blockchain **114** facilitates and stores all the transactions of donations, donors **102** are able to see the details of the registered recipient family **106** in the registered recipient list.

[0051] The public blockchain **114** will store and facilitate transactions for peer-to-peer donations between the donors **102** and the recipient's family **106**. The data in the public blockchain **114** will be accessible to all users of the eGIFT application, guaranteeing transparency in donations.

[0052] In some embodiments, the donor **102** may be provided with tax information option in the browser **104** as shown in **FIG. 8.** The donor **102** may use this option to see different donations that the donor **102** made with for different causes. The donor **102** may also use this information to print a tax benefit report that they can use when filing their tax returns.

[0053] In some embodiments, the donor **102** and the recipient family **106** may access tutorials of the eGIFT application to learn about cryptocurrencies and about how to use the eGIFT application as shown in **FIG. 7**. The donors **102** and recipient family **106** may also receive rewards through the eGIFT application in response to this learning. For example, the tutorials of the eGIFT application may include several topics such as cryptocurrencies, Know you Customer (KYC), helpful resources and the like.

[0054] **FIG.9** shows a block diagram that illustrates the donor searching for a particular cause to provide charities to recipient family **106**, in accordance with some embodiments of the present disclosure. In some embodiments, the donor **102** sends a query to fetch the details of the one or more causes to provide donations to the recipient family **106**. Further, the query is run at the backend and fetches the details from the private consortium blockchain **112** which stores the information of the recipient family **106** and the cause associated with the recipient family **106** as requested by the donor **102**. Upon fetching the details, the response that includes one or more causes is provided to the donor **102**. Finally, the donor **102** may select one or more causes he wishes to donate to one or more recipient families **106**.

[0055] The present disclosure provides several advantages as discussed below:

- a platform to perform a trustworthy, transparent and free of fraud donations given by the donors to the recipients.

- The donors can provide donations using cryptocurrencies directly to the impacted individuals or recipients using cryptocurrency donation service without any friction and full transparency.
- The donors and recipients can use an eGIFT application that uses a decentralized cryptocurrency system. The donors use the eGIFT applications to send the donations through their cryptocurrency wallet directly to the recipients who may need financial assistance.
- Promotes savings and other loyalty benefits.
- The donations performed using blockchain technologies using smart contracts may lead to high efficiency since the transactions takes place as soon as the terms of the contract are met, enhances trustworthiness since the smart contracts are immutable and stored on a federated blockchain, achieves transparency there is no ambiguity as the terms of contract are expressed in computer code and enhances privacy since smart contracts can have variable permission structures, so that only regulators can see the terms of the contract while protecting the identities of the parties themselves.
- Using blockchain technology, the transaction details are transparent, and anyone can see the donations that are being made.
- Members of the consortium blockchain vet recipient credentials. Therefore, fraudsters cannot take advantage of the situation.
- Facilitates real time donations and can be used locally and globally.

[0056] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0057] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g. a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0058] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined based on different embodiments described in the disclosure and/or their equivalents.

[0059] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0060] As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

[0061] 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.

[0062] 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.

[0063] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the disclosure. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

SECURE AND TRUSTWORTHY SYSTEM AND METHOD OF PROVIDING CHARITABLE CONTRIBUTIONS USING CRYPTOCURRENCIES

ABSTRACT

The present disclosure provides a secure and trustworthy system and method of providing charitable contributions using cryptocurrencies. Initially, a registration request may be received from a donor. The request may be received by a node in a private consortium blockchain. Also, a registration request from the recipient family may be received by a node in the private consortium blockchain. The registration request may include sensitive information of the recipient family which is verified by one or more members operating in the private consortium blockchain as being a legitimate recipient family of a charitable donation for a cause. Further, the node of the blockchain network may write a recipient identifier with the cause to the private consortium blockchain. The node of the blockchain network may receive a request to donate an amount of cryptocurrency from the donor to the recipient family. Finally, the node of the blockchain network facilitates a transfer of an amount of cryptocurrency from the donor to the recipient family, which uses a public cryptocurrency blockchain.

FIG. 1

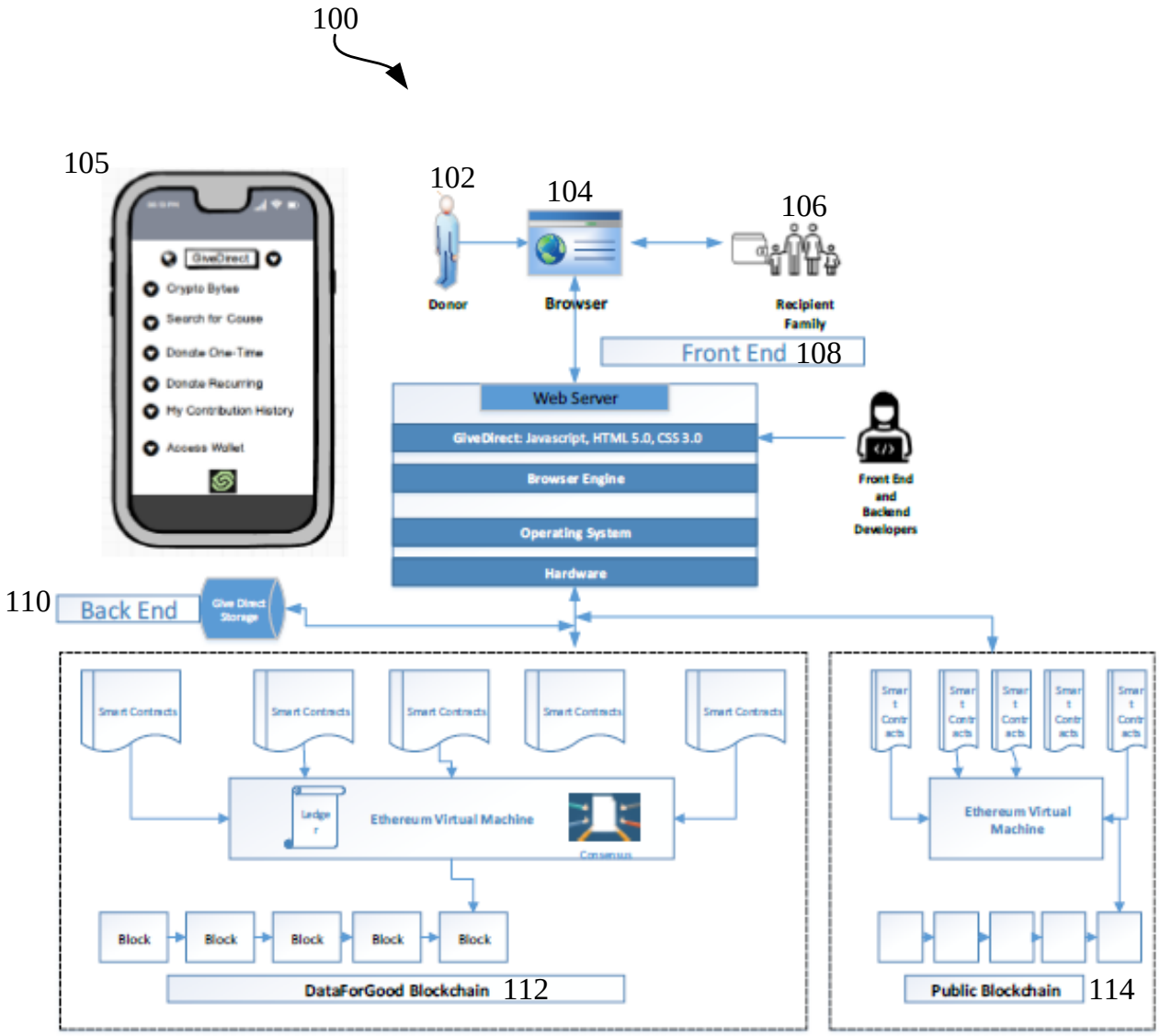

100
105
102
104
106
GiveDirect
Crypto Bytes
Search for Cause
Donate One-Time
Donate Recurring
My Contribution History
Access Wallet
Donor
Browser
Recipient Family
Front End 108
Web Server
GiveDirect: Javascript, HTML 5.0, CSS 3.0
Browser Engine
Operating System
Hardware
Front End and Backend Developers
110
Back End
Give Direct Storage
Smart Contracts
Ledger
Ethereum Virtual Machine
Consensus
Block
DataForGood Blockchain 112
Public Blockchain 114

FIG. 1

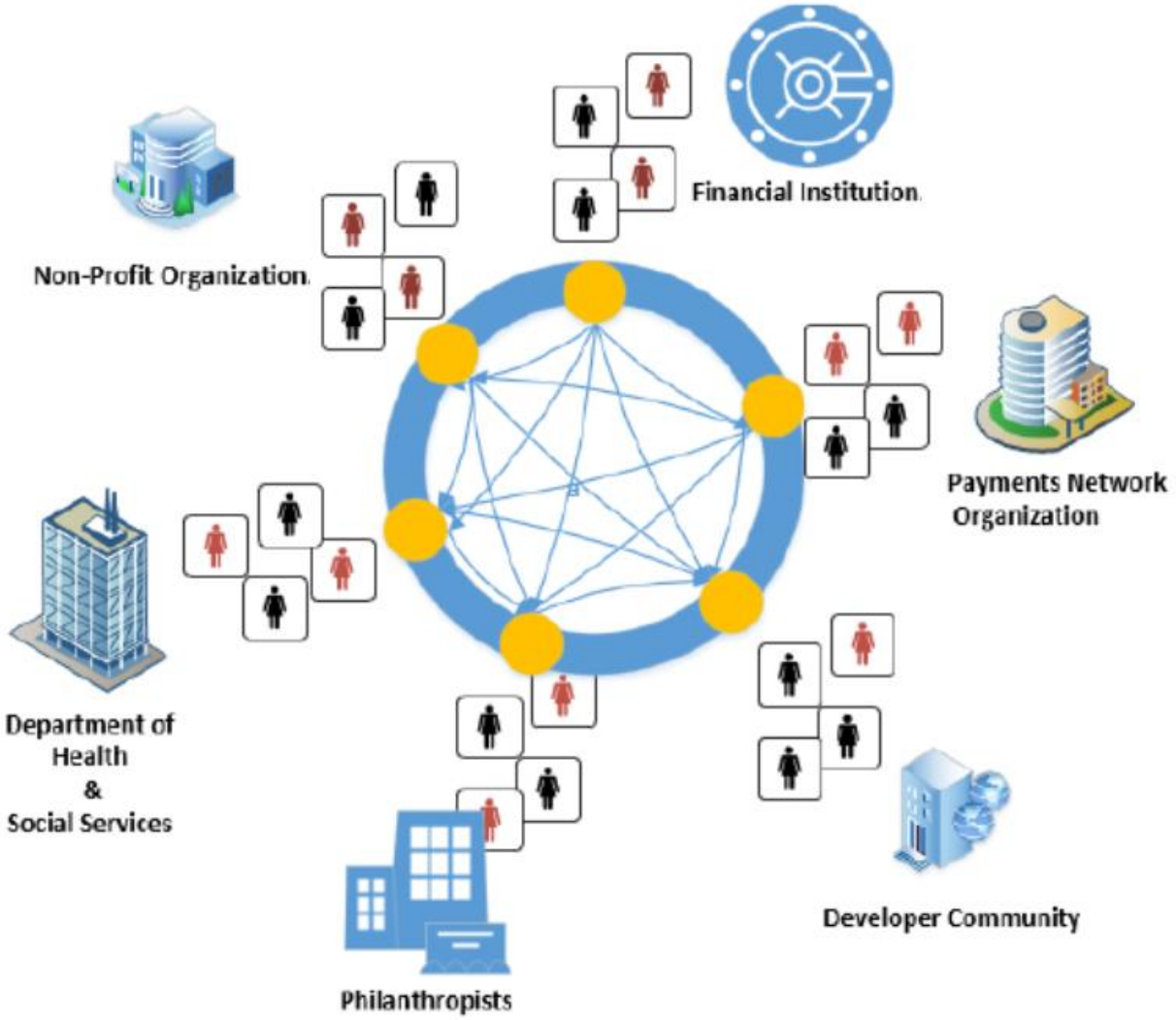

Financial Institution
Non-Profit Organization
Payments Network Organization
Department of Health & Social Services
Developer Community
Philanthropists

FIG. 2

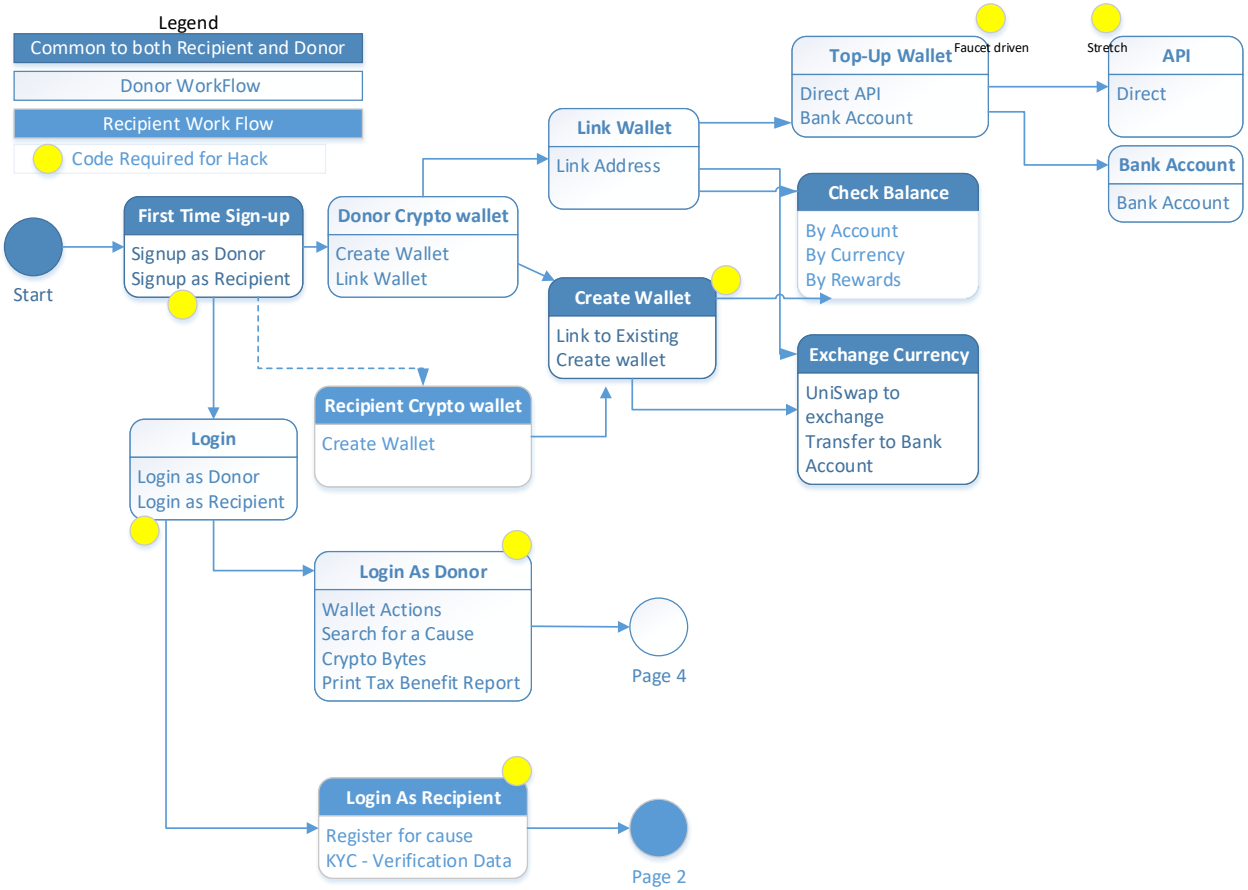

Legend
Common to both Recipient and Donor
Donor WorkFlow
Recipient Work Flow
Code Required for Hack
Start
First Time Sign-up
Signup as Donor
Signup as Recipient
Donor Crypto wallet
Create Wallet
Link Wallet
Link Wallet
Link Address
Top-Up Wallet
Direct API
Bank Account
Faucet driven
Stretch
API
Direct
Bank Account
Bank Account
Check Balance
By Account
By Currency
By Rewards
Create Wallet
Link to Existing
Create wallet
Exchange Currency
UniSwap to exchange
Transfer to Bank Account
Recipient Crypto wallet
Create Wallet
Login
Login as Donor
Login as Recipient
Login As Donor
Wallet Actions
Search for a Cause
Crypto Bytes
Print Tax Benefit Report
Page 4
Login As Recipient
Register for cause
KYC - Verification Data
Page 2

FIG. 3

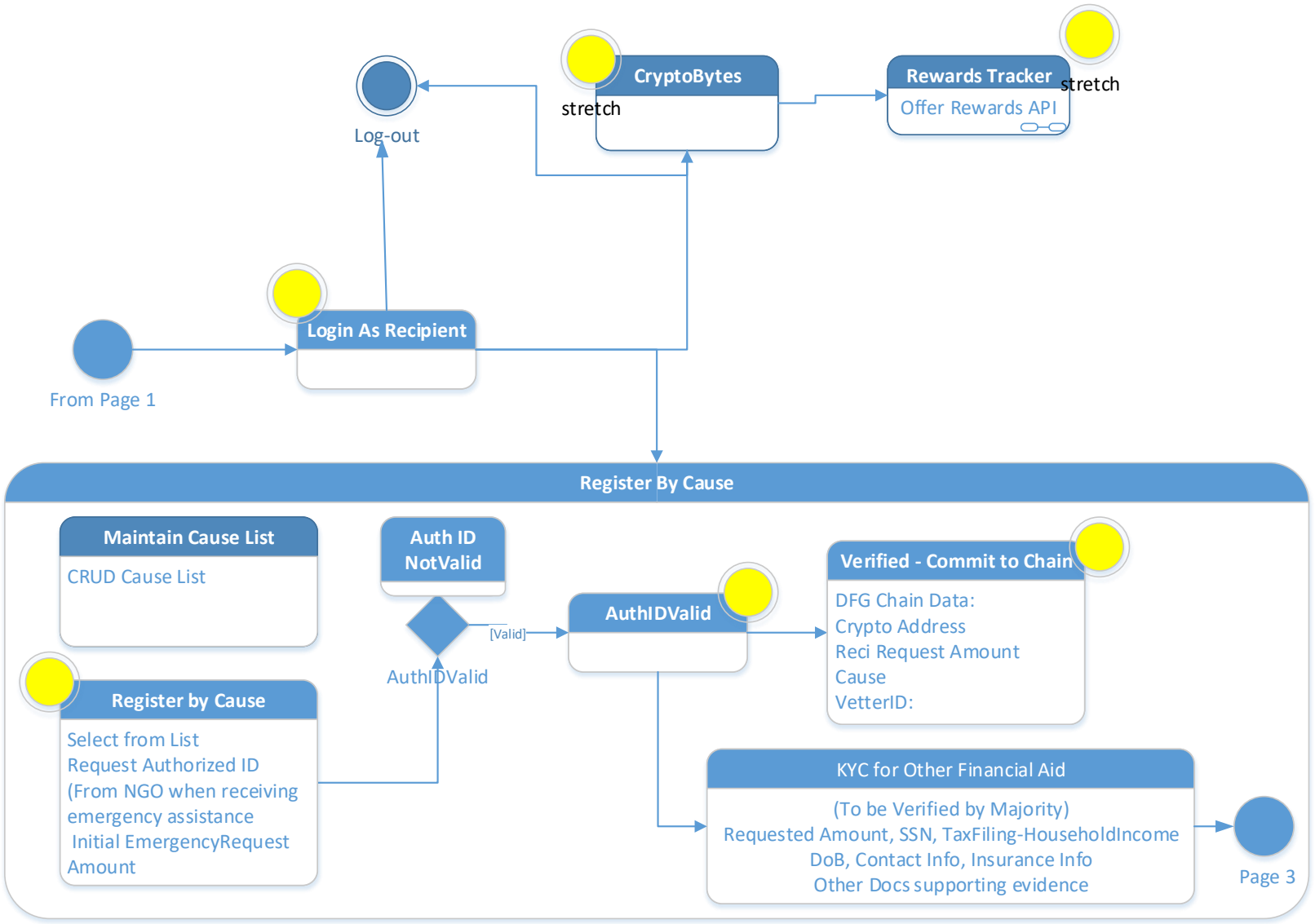

Log-out
CryptoBytes
stretch
Rewards Tracker
stretch
Offer Rewards API
Login As Recipient
From Page 1
Register By Cause
Maintain Cause List
CRUD Cause List
Auth ID NotValid
[Valid]
AuthIDValid
AuthIDValid
Verified - Commit to Chain
DFG Chain Data:
Crypto Address
Reci Request Amount
Cause
VetterID:
Register by Cause
Select from List
Request Authorized ID
(From NGO when receiving emergency assistance
Initial EmergencyRequest Amount
KYC for Other Financial Aid
(To be Verified by Majority)
Requested Amount, SSN, TaxFiling-HouseholdIncome
DoB, Contact Info, Insurance Info
Other Docs supporting evidence
Page 3

FIG. 4

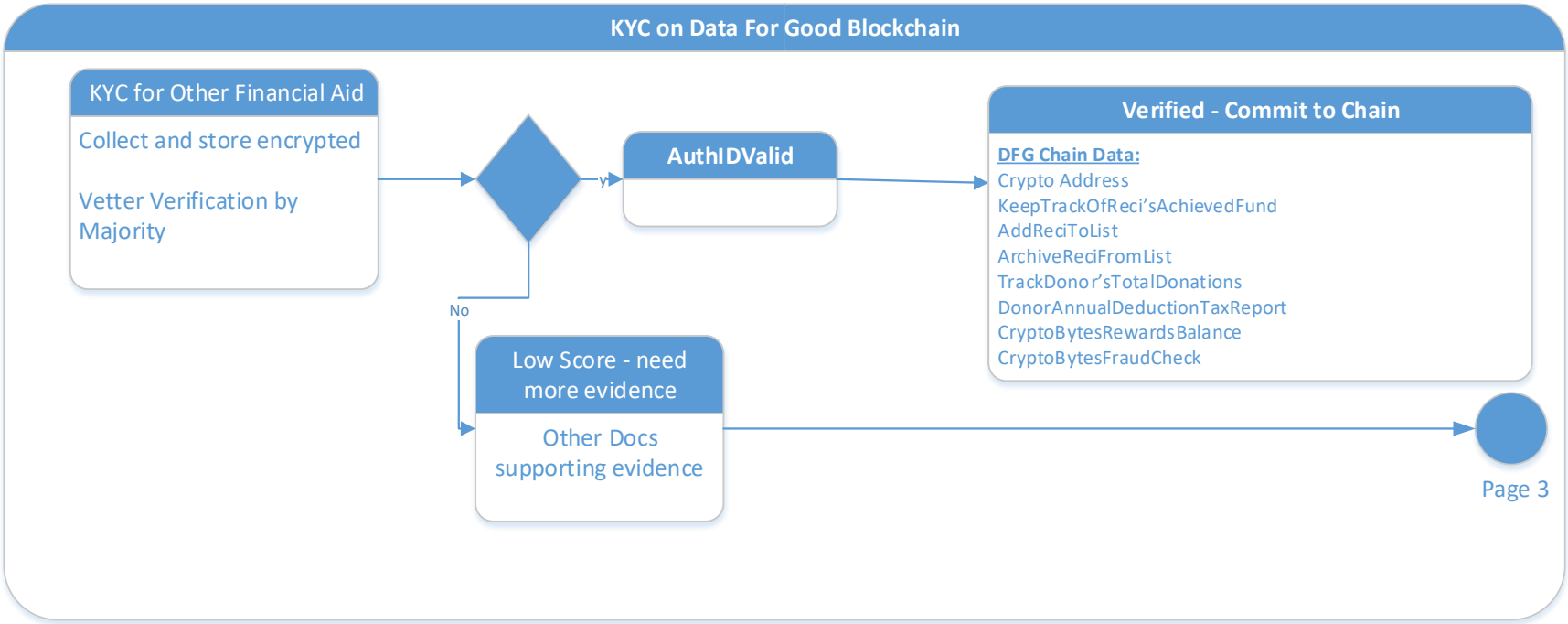

KYC on Data For Good Blockchain
KYC for Other Financial Aid
Collect and store encrypted
Vetter Verification by Majority
Y
AuthIDValid
Verified - Commit to Chain
DFG Chain Data:
Crypto Address
KeepTrackOfReci'sAchievedFund
AddReciToList
ArchiveReciFromList
TrackDonor'sTotalDonations
DonorAnnualDeductionTaxReport
CryptoBytesRewardsBalance
CryptoBytesFraudCheck
No
Low Score - need more evidence
Other Docs supporting evidence
Page 3

FIG. 5

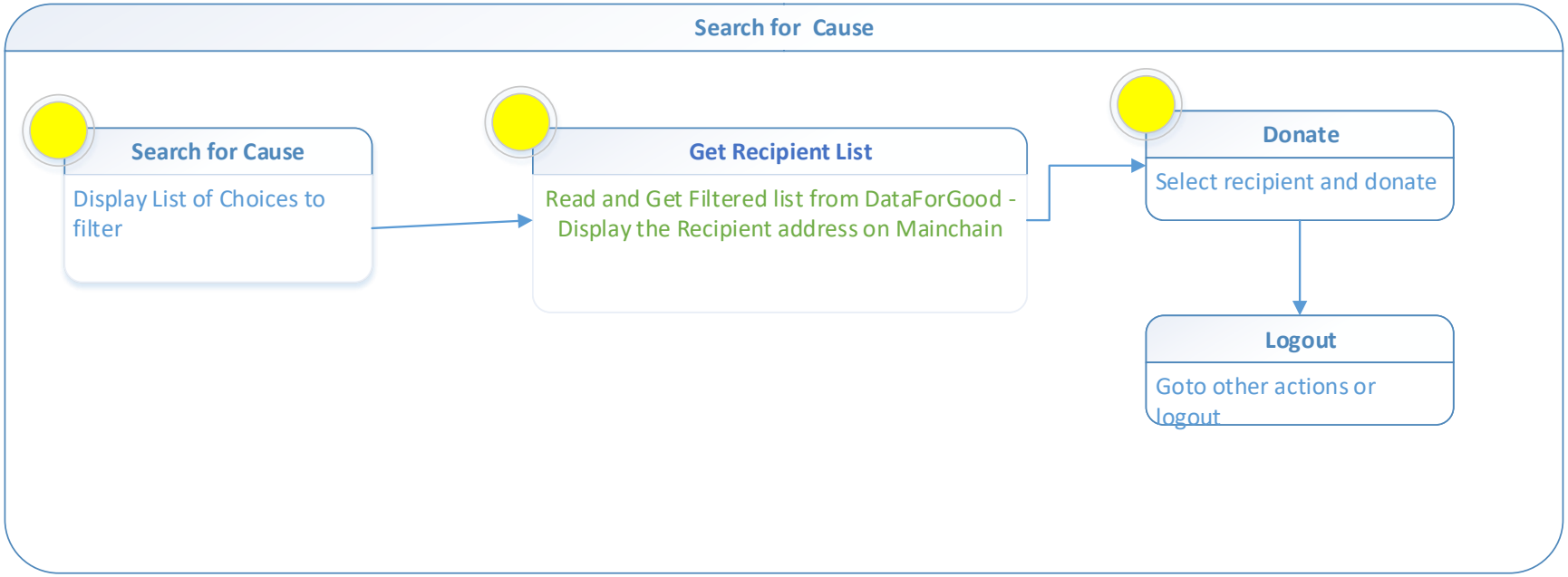
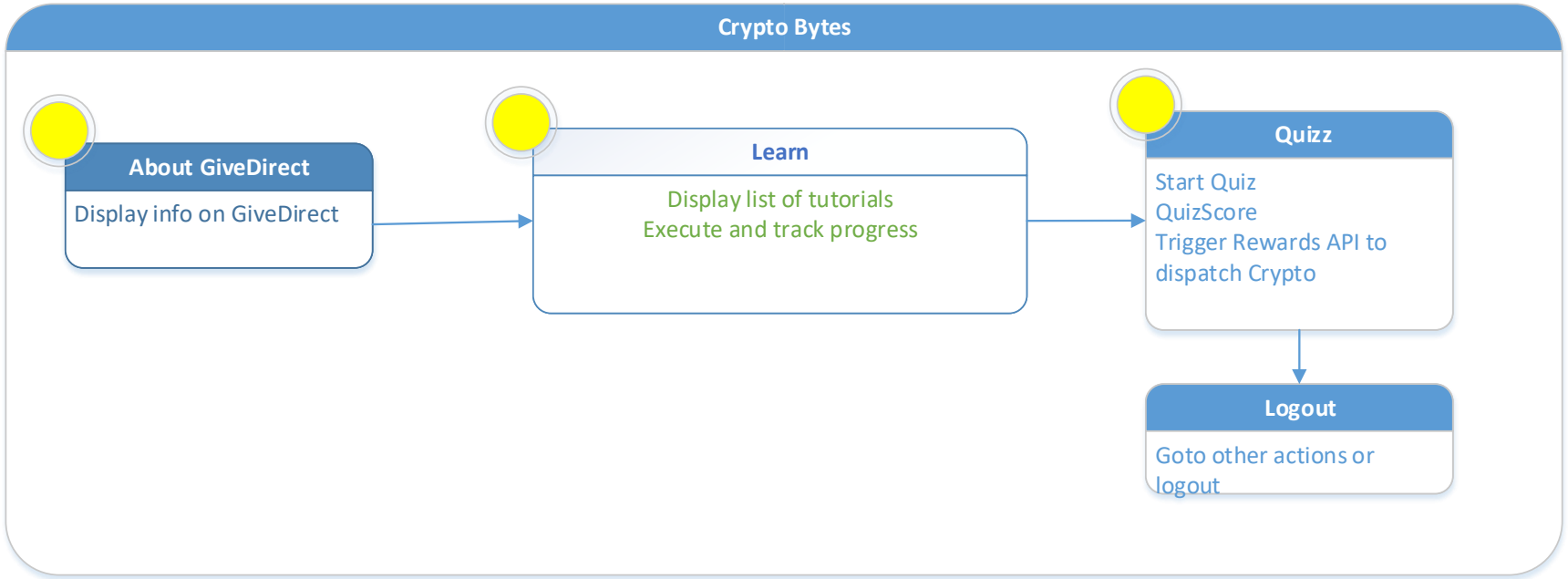

Search for Cause
Search for Cause
Display List of Choices to filter
Get Recipient List
Read and Get Filtered list from DataForGood - Display the Recipient address on Mainchain
Donate
Select recipient and donate
Logout
Goto other actions or logout

FIG. 6


Crypto Bytes
About GiveDirect
Display info on GiveDirect
Learn
Display list of tutorials
Execute and track progress
Quizz
Start Quiz
QuizScore
Trigger Rewards API to dispatch Crypto
Logout
Goto other actions or logout


Crypto Bytes
About GiveDirect
What is Crypto
What is Cryptocurrency
What is KYC
How to Buy and Sell Crypto
Helpful Resources

FIG. 7

Print Tax
Wallet Actions Search for a Cause Crypto Bytes Print Tax Benefit Report

FIG. 8

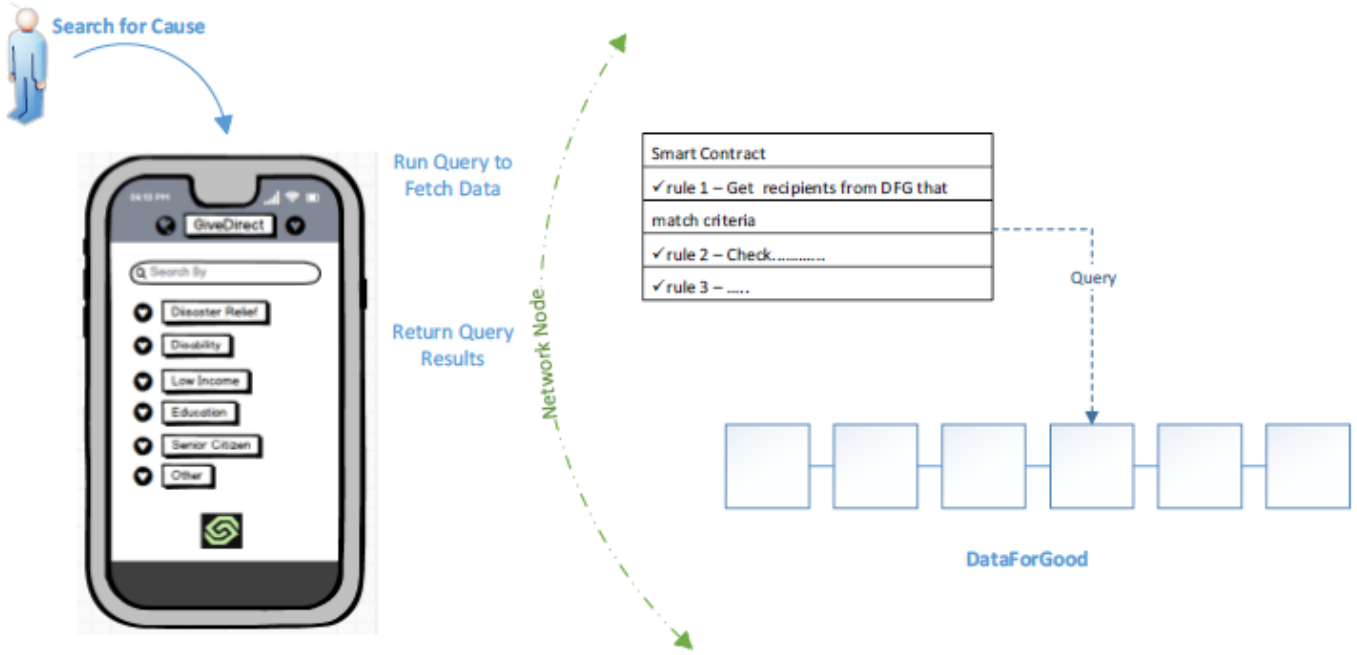


FIG. 9