



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/990,017	05/07/2014		130	COIN-P002Z		

CONFIRMATION NO. 5274

17169
De Klerk & Lundmark
2310 Homestead Road C1 #543
Los Altos, CA 94024

FILING RECEIPT



Date Mailed: 05/19/2014

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Julian Langschaedel, Essen, GERMANY;
Brian D. Armstrong, San Francisco, CA;
Fred E. Ehram, San Francisco, CA;

Applicant(s)

Coinbase, Inc., San Francisco, CA

Power of Attorney:

Stephen De Klerk--46503

If Required, Foreign Filing License Granted: 05/15/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/990,017**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHOD AND SYSTEM FOR TRANSACTING BITCOIN

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Julian

Langschaedel

Inventor 2

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Brian

D.

Armstrong

Inventor 3

Remove

Given Name

Middle Name

Family Name

City

State

Country i

Fred

E.

Ehram

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.**Add****Title of Invention**

A METHOD AND SYSTEM FOR TRANSACTING BITCOIN

Attorney Docket Number (if applicable)

COIN-P002Z

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number☐ Firm or Individual Name

Customer Number

17169

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☒ Yes, applicant qualifies for small entity status under 37 CFR 1.27☐ No**Warning**

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Stephen M. De Klerk/			Date (YYYY-MM-DD)	2014-05-07
First Name	Stephen M.	Last Name	De Klerk	Registration Number (If appropriate)	46503

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	COIN-P002Z
		Application Number	
Title of Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Julian		Langschaedel		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Essen	Country of Residence	DE		
Mailing Address of Inventor:					
Address 1		Diekmannsbusch 10			
Address 2					
City	Essen	State/Province			
Postal Code	45289	Country	DE		
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Brian	D.	Armstrong		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	San Francisco	State/Province	CA	Country of Residence	US
Mailing Address of Inventor:					
Address 1		250 King Street, #1204			
Address 2					
City	San Francisco	State/Province	CA		
Postal Code	94107	Country	US		
Inventor 3					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Fred	E.	Ehram		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	COIN-P002Z
		Application Number	
Title of Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		

Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	San Francisco	State/Province	CA	Country of Residence	US
Mailing Address of Inventor:					
Address 1	935 Sutter Street, #52				
Address 2					
City	San Francisco	State/Province	CA		
Postal Code	94109	Country	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	17169		
Email Address	stephen@dk-lund.com	Add Email	Remove Email
Email Address	ariana.bates@hotmail.com	Add Email	Remove Email

Application Information:

Title of the Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		
Attorney Docket Number	COIN-P002Z	Small Entity Status Claimed	☒
Application Type	Provisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	53	Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.
--

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	COIN-P002Z
		Application Number	
Title of Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	17169		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the application number blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX), the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ¹ (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	COIN-P002Z
		Application Number	
Title of Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices
If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application. In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application. In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	COIN-P002Z
		Application Number	
Title of Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		

Applicant 1			
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section. Clear			
☒ Assignee		☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor :			
If the Applicant is an Organization check here. ☒			
Organization Name	Coinbase, Inc.		
Mailing Address Information For Applicant:			
Address 1	1 Bluxome Street #410		
Address 2			
City	San Francisco	State/Province	CA
Country	US	Postal Code	94107
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.	
Assignee 1	
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.	
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	COIN-P002Z
		Application Number	
Title of Invention	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN		

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		State/Province	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.					
Signature	/Stephen M. De Klerk/			Date (YYYY-MM-DD)	2014-03-17
First Name	Stephen M.	Last Name	De Klerk	Registration Number	46503
Additional Signature may be generated within this form by selecting the Add button.					

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

A METHOD AND SYSTEM FOR TRANSACTING BITCOIN

Inventors: Julian Langschaedel, Brian D. Armstrong and Fred E. Ehram

BACKGROUND OF THE INVENTION

1). Field of the Invention

[0001] This invention relates to a computer system and method for transacting bitcoin.

2). Discussion of Related Art

[0002] The Bitcoin network is a peer-to-peer payment system having a plurality of nodes that are connected to one another. Bitcoin exchange computer systems allow for users to exchange local currency into or out of bitcoin. Users send payments by broadcasting digitally signed messages to the Bitcoin network. Users may, for example, send and receive payments using mobile applications on mobile devices, client software or a web browser.

[0003] Transactions do not explicitly identify the payor and payee by name or wallet. Instead, a bitcoin transaction transfers ownership to a new address, referred to as a “Bitcoin address”. The Bitcoin address is derived from the public portion of one or more cryptographic key pairs. The private portion of a key pair is not disclosed to the public. To send bitcoin sent to an address, a user broadcasts a payment message that is digitally signed with the associated private key.

[0004] Participants known as “miners” at miner computer systems verify and timestamp transactions into a shared public database called a “block chain”. The miners are rewarded with transaction fees and newly minted bitcoin for their effort. The miner computer systems

are specialized computers that append blocks of transactions to the block chain. Solving a cryptographic puzzle required to append a block carries a reward plus fees included in transactions in the block.

[0005] Host computer systems reside at various nodes and may host accounts or “wallets” that allow users to make and accept payments using bitcoin. The wallet stores the public key of the Bitcoin address and its associated private key.

[0006] The transfer of bitcoin may be an onerous task if the entire public key of the Bitcoin address has to be copied and transmitted.

[0007] When a transaction is made between two wallets at the same or different host computer systems, the transaction is broadcast to the Bitcoin network for block chain verification. Such a block chain verification may take a long time to complete. Miner fees are also associated with such a transfer and have to be paid by a host computer system requesting the transfer.

[0008] It may be a security concern for users that their Bitcoin addresses may be stolen from their wallets. Existing systems do not provide a solution for maintaining security of Bitcoin addresses while still allowing the users to use Bitcoin addresses within their wallets for transacting with other users.

SUMMARY OF THE INVENTION

SEND BITCOIN TO EMAIL ADDRESS

[0009] The invention provides a host computer system for transacting bitcoin including a processor, a network interface device connected to the processor, a computer readable medium connected to the processor, a data store on the computer readable medium and a set of instructions on the computer readable medium that are executable by the processor. The set of instructions includes a wallet establishment module, a login module, a hosted email module and a wallet management. The wallet establishment module establishes a first wallet in the data store, stores login details for the first wallet and storing a value representative of an amount of bitcoin held by the first wallet. The login module receives login credentials over the network interface device for the first wallet from a first user device, verifies whether the login credentials match the login details for the first wallet, and if the login credentials match the login details then logs the first user device into the first wallet. The hosted email module, if the first user device is logged into the wallet, permits transmission of an email by a user of the first user device to an email address of a second user device. The wallet management module, in response to the transmission of the email, records a transfer in the first wallet for an amount of bitcoin from the first wallet to a second wallet identified by the email address.

[0010] The invention also provides a method of transacting bitcoin. A processor establishes a first wallet in a data store connected to the processor. The processor stores login details for the first wallet. The processor stores a value representative of an amount of bitcoin held by the first wallet. The processor receives login credentials for the first wallet from a first user device. The processor verifies whether the login credentials match the

login details for the first wallet. The processor, if the login credentials match the login details then, logs the first user device into the first wallet. The processor, if the first user device is logged into the wallet, permits transmission of an email by a user to the first user device to an email address of a second user device and in response to the transmission of the email. The processor records a transfer in the first wallet for an amount of bitcoin from the first wallet to a second wallet identified by the email address.

[0011] The invention further provides a non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor to carry out a method of transacting bitcoin. The processor establishes a first wallet in a data store connected to the processor. The processor stores login details for the first wallet. The processor stores a value representative of an amount of bitcoin held by the first wallet. The processor receives login credentials for the first wallet from a first user device. The processor verifies whether the login credentials match the login details for the first wallet. The processor, if the login credentials match the login details then, logs the first user device into the first wallet. The processor, if the first user device is logged into the wallet, permits transmission of an email by a user to the first user device to an email address of a second user device and in response to the transmission of the email. The processor records a transfer in the first wallet for an amount of bitcoin from the first wallet to a second wallet identified by the email address.

OFF-BLOCK CHAIN TRANSACTIONS IN COMBINATION WITH ON-BLOCK CHAIN TRANSACTIONS

[0012] The invention further provides a first host computer system for transacting bitcoin including a processor at a first node of the Bitcoin network, a network interface device connected to the processor, a computer readable medium connected to the processor, a data store on the computer readable medium and a set of instructions on the computer readable

medium that are executable by the processor. The set of instructions includes a wallet establishment module. The wallet establishment module establishes a first and second wallets in the data store and stores a value representative of an amount of bitcoin held by the first wallet. The wallet management module receives, over the network interface device, a first transfer instruction for an amount of bitcoin from the first wallet and an identifier of the second wallet, in response to the first transfer instruction, records a transfer in the first wallet for the amount of bitcoin in the first transfer instruction out of the first wallet and a transfer in the second wallet, identified by the identifier of the second wallet, for the amount of bitcoin in the first transfer instruction into the second wallet without paying a miner's fee for the first transfer. In order to execute a subsequent on-block chain transaction, the wallet management module receives, over the network interface device, a second transfer instruction for an amount of bitcoin from the first wallet and a bitcoin address associated with a second node of the Bitcoin network, and in response to the second transfer instruction, records a transfer in the first wallet for the amount of bitcoin in the second transfer instruction out of the first wallet, broadcasts a message to the Bitcoin network, including to the second node, to record a transfer associated with the bitcoin address associated with the second node, for the amount of bitcoin in the second transfer instruction, and pays a miner's fee for the second transfer.

[0013] The invention further provides a method of transacting bitcoin including. A processor of a first host computer system at a first node of the Bitcoin network establishes first and second wallets in a data store connected to the processor. The processor stores a value representative of an amount of bitcoin held by the first wallet. The processor receives a first transfer instruction for an amount of bitcoin from the first wallet and an identifier of

the second wallet. The processor, in response to the first transfer instruction, records a transfer in the first wallet for the amount of bitcoin in the first transfer instruction out of the first wallet and a transfer in the second wallet, identified by the identifier of the second wallet, for the amount of bitcoin in the first transfer instruction into the second wallet without paying a miner's fee for the first transfer. The processor receives a second transfer instruction for an amount of bitcoin from the first wallet and a bitcoin address associated with a second node of the bitcoin network. The processor, in response to the second transfer instruction records a transfer in the first wallet for the amount of bitcoin in the second transfer instruction out of the first wallet, broadcasts a message to the Bitcoin network, including to the second node, to record a transfer associated with the bitcoin address associated with the second node, for the amount of bitcoin in the second transfer instruction and pays a miner's fee for the second transfer.

[0014] The invention further provides a non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor of a first host computer system at a first node of the Bitcoin network to carry out a method of transacting bitcoin. The processor establishes first and second wallets in a data store connected to the processor. The processor stores a value representative of an amount of bitcoin held by the first wallet. The processor receives a first transfer instruction for an amount of bitcoin from the first wallet and an identifier of the second wallet. The processor, in response to the first transfer instruction, records a transfer in the first wallet for the amount of bitcoin in the first transfer instruction out of the first wallet and a transfer in the second wallet, identified by the identifier of the second wallet, for the amount of bitcoin in the first transfer instruction into the second wallet without paying a miner's fee for the first transfer. The processor receives

a second transfer instruction for an amount of bitcoin from the first wallet and a bitcoin address associated with a second node of the bitcoin network. The processor, in response to the second transfer instruction records a transfer in the first wallet for the amount of bitcoin in the second transfer instruction out of the first wallet, broadcasts a message to the Bitcoin network, including to the second node, to record a transfer associated with the bitcoin address associated with the second node, for the amount of bitcoin in the second transfer instruction and pays a miner's fee for the second transfer.

BITCOIN PRIVATE KEY SPLITTING FOR COLD STORAGE

[0015] The invention also provides a host computer system for transacting bitcoin including a processor, a computer readable medium connected to the processor, a local storage on the computer readable medium and a set of instructions on the computer readable medium that are executable by the processor. The set of instructions includes a register, a Bitcoin address and an associated private key and value stored in the register, a local controller, a splitter, an offline distribution module, at least one restoration interface, and an assembler. The local controller transfers a private key for a Bitcoin address of a vault, to a local storage connected to a processor and transfers the value of the Bitcoin address in the register to the vault. The splitter splits the private key of the Bitcoin address of the vault into a plurality of codes. The offline distribution module distributes the codes to remote distributed storage locations, removes the private key of the Bitcoin address of the vault from the local storage, and removes the value for the Bitcoin address of the register from the Bitcoin address of the register. The restoration interface receives at least some of the codes into which the private key for Bitcoin address of the vault has been split. The assembler assembles the codes that have been received into the private key of the Bitcoin address of the vault. Th local controller restores the private key of the Bitcoin address of the vault

from the local storage, and restores the value for the Bitcoin address in the register from the vault.

[0016] The invention further provides a method of transacting bitcoin. A processor transfers a private key of the Bitcoin address of a vault to a local storage connected to the processor. The processor splits the private key of the Bitcoin address of the vault into a plurality of codes. The processor distributes the codes to remote distributed storage locations. The processor transfers a value of a Bitcoin address in a register to the vault. The processor receives at least some of the codes into which the private key of the Bitcoin address of the vault has been split. The processor assembles the codes that have been received into the private key of the Bitcoin address of the vault. The processor restores the private key of the Bitcoin address of the vault to the vault. The processor restores the value of the Bitcoin address in the register from the vault.

[0017] The invention also provides a non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor to carry out a method of transacting bitcoin. A processor transfers a private key of the Bitcoin address of a vault to a local storage connected to the processor. The processor splits the private key of the Bitcoin address of the vault into a plurality of codes. The processor distributes the codes to remote distributed storage locations. The processor transfers a value of a Bitcoin address in a register to the vault. The processor receives at least some of the codes into which the private key of the Bitcoin address of the vault has been split. The processor assembles the codes that have been received into the private key of the Bitcoin address of the vault. The processor restores the private key of the Bitcoin address of the vault to the vault. The processor restores the value of the Bitcoin address in the register from the vault.

HOT WALLET FOR HOLDING BITCOIN

[0018] The invention further provides a host computer system for transacting bitcoin including a processor, a network interface device connected to the processor, a computer readable medium connected to the processor, a local storage on the computer readable medium and a set of instructions on the computer readable medium that are executable by the processor. The set of instructions includes a wallet, a plurality of Bitcoin addresses stored in the wallet, a first vault, and a local controller. The local controller is executable for selecting a first transfer set of the Bitcoin addresses for cold storage in the first vault, transferring at least a portion of each of the Bitcoin addresses of the first transfer set to a first vault while keeping the portions a first transaction set in the register, and restoring at least the portion of the Bitcoin addresses of the first transfer set from the first vault to the wallet and a wallet management module transacting using the Bitcoin addresses of the first transacting set without permitting transacting with the Bitcoin addresses of the first transfer set due to the portions thereof being restored to the first vault, and transacting using the Bitcoin addresses of the first transfer set due to the portions thereof being restored from the first vault to the wallet.

[0019] The invention also provides a method of transacting bitcoin. A processor stores a plurality of Bitcoin addresses in a wallet. The processor selects a first transfer set of the Bitcoin addresses for cold storage in a first vault. The processor transfers at least a portion of each of the Bitcoin addresses of the first transfer set to the first vault while keeping the portions a first transaction set in the register. The processor transacts using the Bitcoin addresses of the first transacting set without permitting transacting with the Bitcoin addresses of the first transfer set due to the portions thereof being transferred to the first

vault. The processor restores the portion of the Bitcoin addresses of the first transfer set from the first vault to the wallet. The processor transacts using the Bitcoin addresses of the first transfer set due to the portions thereof being restored from the first vault to the wallet.

[0020] The invention further provides a non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor to carry out a method of transacting. A processor stores a plurality of Bitcoin addresses in a wallet. The processor selects a first transfer set of the Bitcoin addresses for cold storage in a first vault. The processor transfers at least a portion of each of the Bitcoin addresses of the first transfer set to the first vault while keeping the portions a first transaction set in the register. The processor transacts using the Bitcoin addresses of the first transacting set without permitting transacting with the Bitcoin addresses of the first transfer set due to the portions thereof being transferred to the first vault. The processor restores the portion of the Bitcoin addresses of the first transfer set from the first vault to the wallet. The processor transacts using the Bitcoin addresses of the first transfer set due to the portions thereof being restored from the first vault to the wallet.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The invention is further described by way of example with reference to the accompanying drawings, wherein:

[0022] Figure 1A is a block diagram of a network environment that includes the Bitcoin network and a number of systems forming part thereof or connected thereto;

[0023] Figure 1B is a block diagram of a first host computer system and a first and second user devices connected thereto;

[0024] Figure 2 is diagrammatic view of a first wallet that is held within a first host computer system in Figure 1;

[0025] Figure 3 is a view similar to Figure 2, further illustrating a second wallet that has been established within the first host computer system;

[0026] Figure 4 is a view of an email that is received by the second user device in Figure 1;

[0027] Figure 5 is a view of a browser displaying a user interface with fields for creating login details for the second wallet;

[0028] Figures 6 to 30 are views similar to Figure 5 that step a user of the second user device through a wallet set up;

[0029] Figures 31 to 33 are views of the browser wherein the user interface discloses various tools that can be used by the user;

[0030] Figures 34 to 37 are views of the browser wherein the user interface is used by the user to purchase bitcoin from the first host computer system;

[0031] Figure 38 is an email that is received by the second user device to confirm the purchase of the bitcoin from the first host computer system;

[0032] Figure 39 is an email that is received by the second user device with a notification that bitcoin has been added to their wallet as part of a referral bonus system;

[0033] Figure 40 is a view of the browser wherein the user interface displays “Limits and Verifications” associated with the second wallet;

[0034] Figure 41 is a view similar to Figure 3 displaying transfer of bitcoin from the second wallet to the first wallet;

[0035] Figures 42 and 43 are views of the browser when the user interface steps the user through the transfer of bitcoin from the second wallet to the first wallet;

[0036] Figure 44 is a view of the browser wherein the user interface displays Bitcoin addresses associated with transactions that have been completed;

[0037] Figure 45 is a view similar to Figure 40 further showing the transfer of bitcoin from the second wallet to a third wallet that is connected to a second host computer system;

[0038] Figure 46 is a block diagram illustrating splitting of a private key of a vault and offline distribution;

[0039] Figure 47 is a block diagram illustrating removal of the private key of the vault;

[0040] Figure 48 is a block diagram illustrating offline or “cold” storage of values of Bitcoin addresses of a wallet in the vault;

[0041] Figure 49 is a block diagram illustrating isolation of the vault with its private key removed;

[0042] Figure 50 is a block diagram illustrating how the private key of the vault and the value of the Bitcoin addresses are restored;

[0043] Figures 51a to 51d are block diagrams that illustrate how values of certain Bitcoin addresses in a wallet are removed and others are maintained;

[0044] Figure 52 is a graph illustrating how the wallet is maintained within a range so that only a portion of the wallet is “hot” in the sense that a user of the wallet can use the “hot” portion for transacting with another user;

[0045] Figure 53 is a block diagram that shows how an intermediate hot wallet is used to collect value from multiple wallets before transfer to a vault; and

[0046] Figure 54 is a block diagram of a machine in the form of a computer system forming part of the network environment.

DETAILED DESCRIPTION OF THE INVENTION

[0047] Figure 1A of the accompanying drawings illustrates a network environment 10, including the Bitcoin network 12, a first host computer system 14 within which the invention manifests itself, a second host computer system 16, first and second user devices 18 and 20 connected over the Internet 22 to the first host computer system 14, a third user device 24 connected to the second host computer system 16, a bitcoin exchange computer system 26 and a miner computer system 28.

[0048] The Bitcoin network 12 includes a host node 30 and a plurality of remote nodes 32A to D that are connected to one another. The first host computer system 14 is connected to the host node 30. The bitcoin exchange computer system 26 is connected to the remote node 32A. The second host computer system 16 is connected to the remote node 32B. The miner computer system 28 is connected to the remote node 32D or could reside on the same computer system.

[0049] The first host computer system 14 is used primarily for transacting bitcoin and, as shown in Figure 1B, includes a website 34 having a user interface 36, a login module 38, a wallet establishment module 40, a plurality of wallets 42, a wallet management module 44 and a hosted email module 46. The login module 38 is connected to the website 34 and the hosted email module 46 is connected to the login module 38. The wallet establishment module 40 is connected to the wallets 42. The hosted email module 46 is connected via the wallet management module 44 to the wallets 42. As illustrated in the drawing, the first user device 18 is connected over the Internet 22 and the user interface 36 to the login module 38. As further illustrated in the drawing, the hosted email module 46 is connected over the Internet 22 to the second user device 20 and the second user device 20 is connected over the

Internet 22 and the user interface 36 to the wallet establishment module 40.

[0050] As shown in Figure 2, the first host computer system 14 already has one wallet (Wallet A) stored among the wallets 42 corresponding to the first user device 18. The first wallet (Wallet A) includes an email address (email address A) and login details for the wallet. The first wallet (Wallet A) also includes a number of Bitcoin addresses (Bitcoin address 1; Bitcoin address 2) that have been created due to respective transfers or purchases (Transfer 1; Transfer 2). The first Bitcoin address (Bitcoin address 1) is created due to a purchase (Transfer 1) from a master wallet of the first host computer system 14 (First Host) and is recorded for a value in an amount in bitcoin. The second Bitcoin address (Bitcoin address 2) is created due to a transfer (Transfer 2) from another location within the Bitcoin network 12 having a network address outside of the first host computer system 14 and is recorded for a particular amount in bitcoin. The first wallet (Wallet A) was originally established by the wallet establishment module 40 in Figure 1B. The email address (email address A) and login details of the first wallet were also recorded by the wallet establishment module 40. The wallet establishment module 40 and wallet management module 44 were used to record the transfers and purchases (Transfer 1; Transfer 2), their Bitcoin addresses (Bitcoin address 1; Bitcoin address 2), their values and other details within the wallet.

[0051] A user of the first user device 18 in Figure 1B may use a mobile application on the first user device 18 to communicate over the Internet 22 directly with the login module 38 or may use a browser on the first user device 18 to communicate via the Internet 22 and the website 34 with the login module 38. A browser application on the first user device 18 transmits a user interface request over the Internet 22 to the website 34. The website 34

responds to the user interface request by transmitting the user interface 36 over the Internet 22 to the first user device 18. The user interface 36 is then displayed on the first user device 18. The user interface 36 includes fields for entering login credentials, which are then transmitted from the first user device 18 over the Internet 22 to the login module 38. The login module 38 verifies whether the login credentials match the login details for the wallet (Wallet A). If the login credentials match the login details, then the login module 38 logs the first user device 18 into the wallet (Wallet A) in Figure 2. If the login credentials do not match the login details, then the first user device 18 is not logged in to the wallet.

[0052] If the first user device 18 in Figure 1B is logged in to the wallet, the login module 38 also provides access for the first user device 18 to the hosted email module 46 and transmission of an email by a user of the first user device 18 to an email address of the second user device 20. The user interface 36 provides a field for entering the email address of the second user device 20. The user interface 36 also includes a field for entering an amount in bitcoin (or an amount in local currency that is converted to bitcoin using an exchange rate) that is being transferred from the wallet (Wallet A) corresponding to the first user device 18 to a respective wallet among the wallets 42 corresponding to the second user device 20 that has not yet been established at this point in time. The user of the first user device 18 then uses the hosted email module 46 to send an email at 50 to the second user device 20. The hosted email module 46 simultaneously at 52 instructs the wallet establishment module 40 to establish a wallet corresponding to the email address within the wallets 42. The hosted email module 46 simultaneously instructs the wallet management module 44 to record the amount of bitcoin that is being transferred from the wallet (Wallet A) within the wallet corresponding to the email address.

[0053] Figure 3 illustrates further activity within the wallets 42 due to the email represented by a third transfer (Transfer 3). When the user of the first wallet (Wallet A) transmits the email, the system uses an existing Bitcoin address (Bitcoin address 2) to which the outgoing transfer is charged. Associated with the transfer (Transfer 3) are the email address to which the email has been transmitted, the amount in bitcoin, a miner's fee of zero bitcoin that is paid by the first host computer system 14 to any miner computer system such as the miner computer system 28 in Figure 1A, and a host fee of zero bitcoin that are charged to the wallet (Wallet A) for the transfer. A second wallet (Wallet B) is established by the wallet establishment module 40 and the email address (email address B) of the second user device 20 is recorded as an identifier of the wallet (Wallet B). A Bitcoin address (Bitcoin address 3) is recorded within the second wallet (Wallet B) for the transfer (Transfer 3). Within the second wallet (Wallet B), the transfer (Transfer 3) has the Bitcoin address (Bitcoin address 3), the identifier of the wallet (Wallet A) from where the funds are transferred associated therewith, and the amount in bitcoin that has been transferred. The amount in bitcoin corresponding to the transfer (Transfer 3) of both wallets (Wallet A; Wallet B) is the same, consistent with double entry accounting principles. The second wallet (Wallet B) so far has no login details or any other user information and has not been accessed by a user of the second user device 20 at this point in time.

[0054] Figure 4 illustrates the email when it is received at the second user device 20 in Figure 1B. The email is received and viewed within an email application on the second user device 20. The email includes a link ("Click here to sign in and claim this amount") that, when selected by the user of the second user device 20, transmits a user interface request from the browser on the second user device 20 over the Internet 22 to the website 34. The

website 34 responds to the user interface request to transmit the user interface 36 over the Internet 22 to the second user device 20 for viewing within the browser.

[0055] Figure 5 illustrates the user interface 36 as displayed on the second user device 20 in Figure 1B. The user interface 36 includes a plurality of fields for the user of the second user device 20 to enter login details for the second wallet (Wallet B), including a password and a confirmation of the password. After the user has entered a password, the user can access their wallet by selecting the button “Access My Wallet”. The wallet establishment module 40 in Figure 1B stores the login credentials in association with the second wallet (Wallet B). The login module 38 also logs the second user device 20 into the second wallet (Wallet B). If the user is logged out, the user can be provided with a login page where the user can enter login credentials that are compared with the login details in the second wallet (Wallet B) and then log into the second wallet (Wallet B) following a favorable match between the login credentials and the login details.

[0056] Figure 6 shows a view that is displayed on the second user device 20 in Figure 1B. The user is already logged into the wallet, as shown in the top right. The user can accept or decline an agreement. Figure 7 displays the first page that is displayed to the user following acceptance of the agreement. The page shows the current balance corresponding to the amount of bitcoin at the Bitcoin address (Bitcoin address 4) in Figure 3. The user can select various tools down the left margin, including sending or requesting bitcoin, buying or selling bitcoin, account settings and various merchant tools. Figure 8 illustrates a view that is displayed to the user if the user selects the “Buy/Sell” link in Figure 7. The user is prompted to add a bank account. Figures 9 through 15 step the user through the entry of bank account details and verification of the bank account. The user can also select a credit card as a

backup payment. Figures 16 to 19 step the user through the entry of a credit card number and a billing address, and Figures 20 and 21 step the user through a verification process to verify that the user is in control of the credit card account. Figures 22 and 23 request additional information from the user. Figure 23 also allows the user to verify a phone at a phone number and Figures 24 through 27 step the user through a process for verifying their phone and phone number. Figures 28 through 30 illustrate a process for verifying an identity of the user of the second user device 20. As illustrated in Figures 31 to 33, the top margin within the account settings allow for additional tools such as referrals (Figure 31), viewing of Bitcoin addresses (Figure 32), and integration with an application programmable interface (Figure 33).

[0057] Figure 34 illustrates a process that is initiated by the user to purchase bitcoin from a wallet of the first host computer system 14. In the present example, the user selects one (1) bitcoin (BTC) to purchase. Figures 35 and 36 step the user through the process of purchasing the bitcoin. Once the bitcoin is purchased, the user can select on “History” tab in the top margin to display a view as shown in Figure 37 wherein the transaction is displayed and is marked as “PENDING”.

[0058] Figure 38 shows an email that is transmitted by the hosted email module 46 in Figure 1B to the second user device 20 to confirm the purchase of the bitcoin following selection of a “Confirm” button in Figure 35. The email also has a link that, when selected by the user, opens the browser on the second user device 20 and allows the user to login to their wallet and view the transaction.

[0059] Figure 39 shows an email that is transmitted by the hosted email module 46 in Figure 1B to the second user device 20 with a notification that bitcoin has been added to

their wallet as part of a referral bonus system.

[0060] Figure 40 illustrates a view that is displayed when the user selects a “Limits and Verifications” tab in the top margin of the “Buy/Sell” page.

[0061] When the user selects the “Send/Request” link in the left margin in Figure 40, the user is provided an option to send bitcoin from their wallet (Wallet B) in Figure 3 to another wallet (e.g. the first wallet (Wallet A)) in Figure 3.

[0062] Figure 41 illustrates further transfers or purchases (Transfer 4; Transfer 5; Transfer 6). The fourth transfer (Transfer 4) represents the purchase of bitcoin from the first host computer system’s 14 master wallet.

[0063] The fifth transfer (Transfer 5) represents the transfer of bitcoin from the second wallet (Wallet B) to the first wallet (Wallet A). The second wallet (Wallet B) now has login details stored therein. If the second user device 20 in Figure 1B has been logged out of the second wallet (Wallet B), then the second user device 20 is first directed to the login module 38 which receives login details for the second wallet (Wallet B) from the second user device 20, verifies whether the login credentials for the second wallet (Wallet B) match the login details for the second wallet (Wallet B). If the login details match the login credentials, then the login module 38 logs the second user device 20 into the second wallet (Wallet B).

[0064] The login module 38 then provides the second user device 20 with access to the hosted email module 46. The user of the second user device 20 then enters the email address (email address A) of the user of the first wallet (Wallet A) and an amount of bitcoin that the user of the second user device 20 wishes to transfer from the second wallet (Wallet B) to the first wallet (Wallet A). The user of the second user device 20 then uses the hosted email module 46 to send an email via the Internet 22 to the first user device 18. As soon as

the email is sent, a transfer (Transfer 5) is recorded within the second wallet (Wallet B). Because one of the Bitcoin addresses (Bitcoin address 4) has funds associated therewith, it can be charged for the transfer (Transfer 4). Within the second wallet (Wallet B) the transfer (Transfer 4) has the email address (email address A) to which the email has been sent and the amount in bitcoin associated therewith.

[0065] As indicated, the miner's fee that is paid by the first host computer system 14 and the host fee that is charged for the transfer are zero bitcoin because the first wallet (Wallet A) is stored within the wallets 42 of the first host computer system 14. The user of the first user device 18 receives the email indicating the transfer of bitcoin to their wallet (Wallet A). A Bitcoin address (Bitcoin address 5) is recorded within the first wallet (Wallet A) for the transfer (Transfer 5) together with the identifier of the second wallet (Wallet B) from which the transfer has been made and the amount in bitcoin. The amount in bitcoin corresponding to the transfer (Transfer 4) in the second wallet (Wallet B) is the same as the amount in bitcoin as in the first wallet (Wallet A).

[0066] As illustrated by the next transfer (Transfer 6), the user of the second wallet (Wallet B) can opt to send bitcoin to a Bitcoin address of the first wallet (Wallet A). The transfer (Transfer 6) is the same as the preceding transfer (Transfer 5) in all other respects.

[0067] Figure 42 shows a view that is displayed to the user of the second user device 20 in Figure 1B in order to make the transfer from their wallet (Wallet B) to the first wallet (Wallet A). The view includes a field for the user to enter the email address (email address A) and fields for entering either an amount in bitcoin (BTC) or an amount in a local currency (USD-United States Dollar). The exchange rate between bitcoin and the local currency is shown in the top left corner. The view also includes a button "Send Money"

which, when selected by the user, initiates the transfer of bitcoin.

[0068] Figure 43 is a view that is displayed to the user indicating transactions that have been initiated or completed. The purchase of bitcoin discussed with reference to Figures 35 to 37 is shown as “PENDING”. A block chain verification notice has to be broadcast by the miner computer system 28 and be received by the first host computer system 14 in Figure 1A before a determination is made to change the marker “PENDING” to “COMPLETE”. The other transactions representing transfers between the first and second wallets (Wallet A and Wallet B) in Figure 41 are shown as completed because they do not need block chain verification outside of the first host computer system 14. No block chain verification notice is thus required for these transactions to be marked “COMPLETE”. Figure 44 shows a view that can be selected by the user by selecting a tab in the top margin wherein the user is shown the Bitcoin addresses associated with transactions that have been completed.

[0069] Figure 45 illustrates a further transaction (Transfer 7) wherein bitcoin is transferred from the second wallet (Wallet B) to a third wallet (Wallet C) held by the second host computer system 16 in Figure 1A. The user of the second user device 20 enters a bitcoin address (Bitcoin address 6) that is located in the third wallet (Wallet C) and an amount of bitcoin to be transferred to the third wallet (Wallet C). A transfer (Transfer 7) is recorded within the second wallet (Wallet B). Associated with the transfer (Transfer 7) are the Bitcoin address (Bitcoin address 6), the amount in bitcoin that is being transferred and a miner’s fee that is charged for the transfer and has to be paid by the first host computer system 14 to the miner computer system 28 in Figure 1A. No fee is charged by the first host computer system 14 for a transfer to another Bitcoin address.

[0070] When the user of the second user device 20 in Figure 1A completes the purchase, a

transfer instruction is created and is broadcast via the host node 30 to all remote nodes 32A-D within the Bitcoin network 12. The transfer instruction thus traverses the first node and the second remote node 32B to reach the second host computer system 16. The second host computer system 16 and all other computer systems connected to the remote nodes 32A-D record the transfer (Transfer 7) with respect to the Bitcoin addresses (Bitcoin address 4; Bitcoin address 6). The transfer (Transfer 7) has associated therewith the amount in bitcoin.

[0071] The transfer instruction that results in the transfer (Transfer 5) thus results in no miner's fee being charged to and paid by the first host computer system 14. No host fee is charged to the second wallet (Wallet B) because the transfer (Transfer 7) is made to another wallet (Wallet A) within the wallets 42 of the first host computer system 14. By contrast, the transfer instruction that results in the transfer (Transfer 7) representing the transfer to the Bitcoin address (Bitcoin address 6) in the third wallet (Wallet C) results in a miner's fee that is paid by the first host computer system 14 to the miner computer system 28. The miner computer system 28 is responsible for verifying transfers of bitcoin over the Bitcoin network 12. In the present scenario, the miner computer system 28 verifies the transfer of bitcoin from the second wallet (Wallet B) to the third wallet (Wallet C).

[0072] Another transfer may comprise that bitcoin is sent to one of the nodes, e.g. node 32C. The node 32C could be a fourth user device which is owned by the recipient of the bitcoin transfer having its own bitcoin address.

[0073] Figure 46 illustrates components that are used for cold storage of value of bitcoin, including a local storage 56, a local controller 58, a vault 64, a splitter 66, one or more encryption algorithms 68 and 70 and an offline distribution module 72.

[0074] The vault 64 has a Bitcoin address 80 with a private key 79. The private key 79 is,

for purposes of illustration, shown as a nine digit sequence of characters that are provided to the splitter 66. For purposes of illustration, the splitter 66 splits the nine digits of the private key 79 into seven overlapping codes (Codes 1 to 7). The encryption algorithm 68 encrypts the first code (Code 1) into an encrypted code (Encrypted Code 1). In a similar manner, the second code (Code 2) is encrypted by an encryption algorithm (not shown) into an encrypted code (Encrypted Code 2). Each one of the seven codes is encrypted into a separate encrypted code. A separate key may be used for each one of seven codes. Alternatively, a separate encryption algorithm may be used for each one of the seven codes.

[0075] Once all the codes have been encrypted, the offline distribution module 72 transmits each one of the encrypted codes (Encrypted Code 1 to 7) to a separate location. The locations are remote locations that are geographically separated from one another. The offline distribution module 72 may also be used to print one or more of the encrypted codes for paper delivery to respective remote locations.

[0076] Figure 47 illustrates functioning of the offline distribution module 72 following distribution of the encrypted codes in Figure 46. The offline distribution module 72 removes the private keys 79 of the Bitcoin address 80 of the vault 64. The offline distribution module 72 also removes the private key 79 of the Bitcoin address 80 within the local storage 56.

[0077] As shown in Figure 48, a local register 60 includes a plurality of wallets 42, one of which is shown. The wallet 42 has a plurality of Bitcoin addresses 74, 76 and 78 associated therewith. Each Bitcoin address 74, 76 and 78 has a respective value and a respective private key. The local controller 58 transfers the entire value of the Bitcoin addresses 76 and 78 into the vault 64. The value relating to the Bitcoin address 74 is not transferred into

the vault 64. The local controller 58 calculates the total value of the Bitcoin addresses 76 and 78 that have been transferred into the vault 64 and records the total value in the local storage 56 in association with the Bitcoin address 80.

[0078] As shown in Figure 49, following removal of the value of the Bitcoin addresses 76 and 78 within the wallet 42, the value of the Bitcoin addresses 76 and 78 are only held within the vault 64 and the local storage 56. The private key 79 is only held in a split and encrypted form at the distributed locations where the offline distribution module 72 in Figure 46 has distributed them to. Unless access can be gained to the private key 79 that has now been split and distributed, it is not possible to access the value of the Bitcoin addresses 76 and 78. It is now possible for a user to which the wallet 42 is registered to use the Bitcoin address 74 for transacting with another user via the wallet management module 40 in Figure 1B. The Bitcoin addresses 76 and 78 are not usable by the wallet management module 40 for purposes of transacting with another user at this time because their values, within the wallet 42, have been removed.

[0079] Figure 50 shows how the private keys of the vault 64 and the Bitcoin addresses 76 and 78 that were removed in Figure 46 are restored. Components that are provided for restoration include a plurality of restoration interfaces 82, 84 and 86, one or more decryption algorithms 88, 90 and 92 and an assembler 94. The holder of the first encrypted code (Encrypted Code 1) is called upon to enter the encrypted code into the restoration interface 82. The restoration interface 82 may for example be a web page with a field for entry of the first encrypted code. Alternatively, the restoration interface 82 may be an application programmable interface (API) and the first encrypted code can be entered into the API with or without human involvement.

[0080] In the given example, the second, third, fifth and sixth encrypted codes are not received at this time. The fourth and seventh encrypted codes are received through the restoration interfaces 84 and 86, similar to the first encrypted code.

[0081] The decryption algorithm 88 decrypts the first encrypted code (Encrypted Code 1) into the first code (Code 1). In the given example, the decryption algorithms 90 and 92 decrypt the fourth and seventh encrypted codes (Encrypted Code 4 and Encrypted Code 7) into the fourth and seventh codes (Code 4 and Code 7) respectively. In the given example, three codes are the minimum number of codes that are required in order to reassemble the private key 79. The minimum number of codes required for reassembly in Figure 48 is thus less than the total number of codes into which the private key 79 has been split in Figure 46. The assembler 94 assembles the private key 79 when the minimum number of codes has been received.

[0082] The private key 79 of the Bitcoin address 80 in the local storage 56 is used to access the vault 64. The local controller 58 then restores the private key 79 from the local storage into the vault for association with the Bitcoin address. The block chain will know whether the private key 79 that has been restored is the same private key 79 that was previously associated with the Bitcoin address. Only upon confirmation from the block chain will it be possible to transfer the value from the vault 64 to the local register 60.

[0083] The local controller 58 restores the respective value of the Bitcoin addresses 76 and 78 in the vault 64 to the Bitcoin addresses 76 and 78 in the wallet 42. Because the values have been restored to the Bitcoin addresses 76 and 78 in the wallet 42 they are usable for transacting with other users.

[0084] Figures 51a to 51d illustrate the use of a “hot” wallet in combination with “cold

storage”. As shown in Figure 51a, the wallet 42 has the Bitcoin addresses 74, 76, 78 and a further Bitcoin address 98, each having a respective value associated therewith. The local storage 56 has first, second and third Bitcoin addresses 80A to 80C for first, second and third vaults 64A to 64C, respectively. The Bitcoin addresses 76 and 78 form a first transfer set that is selected for cold storage. The Bitcoin addresses 74 and 98 form a first transacting set. The values of the Bitcoin addresses 76 and 78 of the first transfer set are transferred into the first vault 64A, as represented by “Value” in the first vault 64A.

[0085] The private key of the Bitcoin address 80A of the first vault 64A is then transferred into the local storage 56 and is stored in association with the first Bitcoin address 80A. As hereinbefore described with reference to Figure 46, the private key of the Bitcoin address 80A in the local storage 56 is then split and distributed. As hereinbefore described with reference to Figure 47 and 48, the private keys of the Bitcoin address 80 and the value of the Bitcoin address 76 and 78 are then removed. It is then not possible for a user of the wallet 42 to use the Bitcoin address 76 and 78 for transacting with another user. The user can still transact with another user using the Bitcoin addresses 74 and 98 of the first transacting set because their values are still associated with them within the wallet 42.

[0086] Figure 51b shows the Bitcoin addresses 76 and 78 within the wallet 42 with their values removed and the Bitcoin address 80A within the local storage 56 with its private key removed. The private key of the Bitcoin address 80B of second vault 64B is transferred into the local storage 56 and associated with the second Bitcoin address 80B within the local storage 56. The private key of the second Bitcoin address 80B in the local storage 56 is split and distributed and then removed from the local storage 56. The Bitcoin address 98 is selected as part of a second transfer set of one or more Bitcoin addresses. The value of the

Bitcoin address 98 is transferred from the wallet 42 into the second vault 64B, as represented by “Value” in the second vault 64B. The value of the Bitcoin address 98 within the wallet 42 is thus removed. The user of the wallet 42 can now not use the Bitcoin address 98 for purposes of transacting with another user because the value of the Bitcoin address 98 has been removed from the wallet 42. The Bitcoin address 74 forms part of a second transacting set that may include one or more Bitcoin addresses that can be used for transacting with another user.

[0087] Figure 51c shows the Bitcoin address 98 having its value removed and the second Bitcoin address 80B within the local storage 56 having its private key removed. At this stage it may be desirable to restore the values of the Bitcoin addresses 76 and 78. The private key of the first Bitcoin address 80A within the local storage 56 is restored to the vault 64 as hereinbefore described with reference to Figure 50. The respective values of the Bitcoin addresses 76 and 78 are then restored from the vault 64A to the Bitcoin addresses 76 and 78 in the wallet 42. Because the values of the Bitcoin addresses 76 and 78 are restored within the wallet 42, the Bitcoin addresses 76 and 78 of the first transfer set can, at least for the time being, be used together with the second transacting set for transacting with another user.

[0088] The same Bitcoin addresses 74, 76, 78 and 98 that are shown in Figure 51a are also shown in Figure 51b and 51c. It should be understood that the Bitcoin addresses may change between the figures. The system allows for the value that was previously associated with one Bitcoin address to be restored to another Bitcoin address if necessary.

[0089] As shown in Figure 51d, the first vault 64A is discarded after the value therein is restored. The first Bitcoin address 80A within the local storage 56 and the first vault 64A

will never be used again.

[0090] The Bitcoin address 78 is selected as a third transfer set. The private key of the Bitcoin address 80C of the third vault 64C is transferred into the local storage 56 and stored in association with a third Bitcoin address 80C. The value of the Bitcoin address 78 is transferred from the wallet 42 to the third vault 64C. The user of the wallet 42 can now not use the Bitcoin address 78 for transacting with another user. The Bitcoin address 76 forms part of a third transacting set that could include one or more Bitcoin addresses. The Bitcoin address 76 can be used by the user of the wallet 42 for transacting with another user because the value of the Bitcoin address 76 is associated therewith within the wallet 42. The second and third transacting sets can thus be used by the user for transacting with another user. The second and third transfer sets are unusable for transacting with another user because their private keys have been removed.

[0091] Figure 52 illustrates how the local controller 58 (see Figures 46 to 50) maintains transaction sets of a wallet 42 within a target range 101. Should all the Bitcoin addresses of the wallet 42 have values associated therewith, the wallet 42 is said to be 100% hot and 0% cold. If all the Bitcoin addresses in a wallet 42 have their values removed, the wallet 42 is to be 0% hot and 100% cold. The target range 101 for the total bitcoin value within the wallet may for example be 5% to 10% hot. At 102, the values of the first transacting set are transferred from the wallet 42 as described with reference to Figure 51a. At 104, the user transacts with some of the Bitcoin addresses and the total value within the wallet 42 of the Bitcoin addresses that are hot is reduced. At 106, the values of the second transfer set are removed from the wallet 42 as described with reference to Figure 51b. At 108, the values of the first transfer set are restored as described with reference to Figure 51c. At 110, the user

transacts and gains further Bitcoin addresses for additional value within their wallet 42. At 112, values of the third transfer set are transferred out of the wallet 42 as described with reference to Figure 51d. It can thus be seen that the local controller 58 in Figure 46 to 50 adjusts the total value of bitcoin that is not within the target range 101. The local controller 58 typically recalculates the hot/cold value ratio of each wallet on a daily basis and automatically adjusts the value to the target range 101.

[0092] Figure 53 illustrates the use of an intermediate hot wallet 114 that is used to collect bitcoin values from a plurality of wallets 42A to C. The wallet 42A is that same as the wallet 42 as described above. The wallet 42B has bitcoin addresses 120, 122, 124 and 126 associated therewith. The wallet 42C has bitcoin addresses 128, 130, 132 and 134 associated therewith. Each wallet 42A, B or C is held within the target range 101 in Figure 50. The values of the bitcoin addresses 76, 78, 120, 122, 128 and 130 are identified for transfer to the vault 64A and are first transferred or “swept” to the intermediate hot wallet 114 from where they are transferred to the vault 64A.

[0093] Figure 54 shows a diagrammatic representation of a machine in the exemplary form of a computer system 900 within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine operates as a standalone device or may be connected (e.g., networked) to other machines. In a network deployment, the machine may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a network router, switch or bridge, or any

machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term “machine” shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0094] The exemplary computer system 900 includes a processor 930 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), or both), a main memory 932 (e.g., read-only memory (ROM), flash memory, dynamic random access memory (DRAM) such as synchronous DRAM (SDRAM) or Rambus DRAM (RDRAM), etc.), and a static memory 934 (e.g., flash memory, static random access memory (SRAM), etc.), which communicate with each other via a bus 936.

[0095] The computer system 900 may further include a video display 938 (e.g., a liquid crystal displays (LCD) or a cathode ray tube (CRT)). The computer system 900 also includes an alpha-numeric input device 940 (e.g., a keyboard), a cursor control device 942 (e.g., a mouse), a disk drive unit 944, a signal generation device 946 (e.g., a speaker), and a network interface device 948.

[0096] The disk drive unit 944 includes a machine-readable medium 950 on which is stored one or more sets of instructions 952 (e.g., software) embodying any one or more of the methodologies or functions described herein. The software may also reside, completely or at least partially, within the main memory 932 and/or within the processor 930 during execution thereof by the computer system 900, the memory 932 and the processor 930 also constituting machine readable media. The software may further be transmitted or received over a network 954 via the network interface device 948.

[0097] While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative and not restrictive of the current invention, and that this invention is not restricted to the specific constructions and arrangements shown and described since modifications may occur to those ordinarily skilled in the art.

CLAIMS

What is claimed:

SEND BITCOIN TO EMAIL ADDRESS

Inventor: Brian D. Armstrong

1. A host computer system for transacting bitcoin comprising:
 - a processor;
 - a network interface device connected to the processor;
 - a computer readable medium connected to the processor;
 - a data store on the computer readable medium; and
 - a set of instructions on the computer readable medium that are executable by the processor, including:
 - a wallet establishment module establishing a first wallet in the data store, storing login details for the first wallet and storing a value representative of an amount of bitcoin held by the first wallet;
 - a login module receiving login credentials over the network interface device for the first wallet from a first user device, verifying whether the login credentials match the login details for the first wallet, and if the login credentials match the login details then logging the first user device into the first wallet;
 - a hosted email module that, if the first user device is logged into the wallet, permits transmission of an email by a user of the first user device to an email address of a second user device; and

a wallet management module that, in response to the transmission of the email, records a transfer in the first wallet for an amount of bitcoin from the first wallet to a second wallet identified by the email address.

2. The host computer system of claim 1, wherein the set of instructions further includes:

a website receiving a user interface request from the first user device over the network interface device; and

a user interface of the website that is transmitted over the network interface device in response to the user interface request from the first user device, the user interface having at least one field for entering the login credentials and a field for entering the email address.

3. The host computer system of claim 2, wherein the user interface includes a field for entering of the amount of bitcoin that is being transferred.

4. The host computer system of claim 1, wherein the second wallet is stored in the data store connected to the processor.

5. The host computer system of claim 4, wherein the wallet management module, in response to the transmission of the email, records the transfer in the second wallet.

6. The host computer system of claim 4, wherein the wallet establishment module, in response to the transmission of the email, creates and stores the second wallet in the data store connected to the processor.

7. The host computer system of claim 6, wherein the email includes a link that, when selected by a user of the second user device, transmits a user interface request from a browser of the second user device, further comprising:

a website receiving the user interface request from the second user device over the network interface device; and

a user interface of the website that is transmitted over the network interface device in response to the user interface request from the second user device, the user interface having a plurality of fields for the user of the second user device to enter at least login details for the second wallet, wherein the wallet establishment module stores the login details received from the second user device in association with the second wallet.

8. The host computer system of claim 7, wherein the login module stores login details for the second wallet, receives login credentials for the second wallet from a second user device, verifies whether the login credentials for the second wallet match the login details for the second wallet, and if the login credentials match the login details then logs the second user device into the second wallet, and if the second user device is logged into the wallet, displays the amount of bitcoin being transferred.

9. The host computer system of claim 4, wherein the second wallet includes a plurality of Bitcoin addresses wherein each Bitcoin address represents a respective transfer of bitcoin to the second wallet.

10. A method of transacting bitcoin comprising:

establishing, by a processor, a first wallet in a data store connected to the processor;

storing, by the processor, login details for the first wallet;

storing, by the processor, a value representative of an amount of bitcoin held by the first wallet;

receiving, by the processor, login credentials for the first wallet from a first user device;

verifying, by the processor, whether the login credentials match the login details for the first wallet;

if the login credentials match the login details then, by the processor, logging the first user device into the first wallet;

if the first user device is logged into the wallet, permitting, by the processor, transmission of an email by a user to the first user device to an email address of a second user device; and

in response to the transmission of the email, recording, by the processor, a transfer in the first wallet for an amount of bitcoin from the first wallet to a second wallet identified by the email address.

11. The method of claim 10, further comprising:

receiving, by the processor, a user interface request at a website from the first user device; and

transmitting, by the processor in response to the user interface request, a user interface of the website to the first user device, the user interface having at least one field for entering the login credentials and a field for entering the email address.

12. The method of claim 11, wherein the user interface includes a field for entering of the amount of bitcoin that is being transferred.

13. The method of claim 10, wherein the second wallet is stored in the data store connected to the processor.

14. The method of claim 13, further comprising:

in response to the transmission of the email, recording, by the processor, the transfer in the second wallet.

15. The method of claim 13, further comprising:

in response to the transmission of the email, creating and storing, by the processor, the second wallet in the data store connected to the processor.

16. The method of claim 15, wherein the email includes a link that, when selected by a user of the second user device, transmits a user interface request from a browser of the second user device, further comprising:

receiving, by the processor, a user interface request at a website from the second user device;

transmitting, by the processor in response to the user interface request, a user interface of the website to the first user device, the user interface having a plurality of fields for the user of the second user device to enter at least login details for the second wallet; and

storing the login details received from the second user device in association with the second wallet.

17. The method of claim 16, further comprising:

receiving, by the processor, login credentials for the second wallet from a second user device;

verifying, by the processor, whether the login credentials match the login details for the second wallet;

if the login credentials for the second wallet match the login details then, by the processor, logging the second user device into the second wallet; and

if the second user device is logged into the wallet, displaying, by the processor, the amount of Bitcoin being transferred.

18. The method of claim 13, wherein the second wallet includes a plurality of Bitcoin addresses wherein each Bitcoin address represents a respective transfer of bitcoin to the second wallet.

19. A non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor to carry out a method of transacting bitcoin comprising:

establishing, by a processor, a first wallet in a data store connected to the processor;

storing, by the processor, login details for the first wallet;

storing, by the processor, a value representative of an amount of Bitcoin held by the first wallet;

receiving, by the processor, login credentials for the first wallet from a first user device;

verifying, by the processor, whether the login credentials match the login details for the first wallet;

if the login credentials match the login details then, by the processor, logging the first user device into the first wallet;

if the first user device is logged into the wallet, permitting, by the processor, transmission of an email by a user to the first user device to an email address of a second user device; and

in response to the transmission of the email, recording, by the processor, a transfer in the first wallet for an amount of bitcoin from the first wallet to a second wallet identified by the email address.

OFF-BLOCK CHAIN TRANSACTIONS IN COMBINATION WITH ON-BLOCK CHAIN TRANSACTIONS

Inventor: Brian D. Armstrong

20. A first host computer system computer system for transacting bitcoin comprising:
a processor at a first node of the Bitcoin network;
a network interface device connected to the processor;
a computer readable medium connected to the processor;
a data store on the computer readable medium; and
a set of instructions on the computer readable medium that are executable by the processor, including:

a wallet establishment module establishing a first and second wallets in the data store, storing a value representative of an amount of bitcoin held by the first wallet;
and

a wallet management module receiving, over the network interface device, a first transfer instruction for an amount of bitcoin from the first wallet and an identifier of the second wallet, in response to the first transfer instruction, recording a transfer in the first wallet for the amount of bitcoin in the first transfer instruction out of the first wallet and a transfer in the second wallet, identified by the identifier of the second wallet, for the amount of bitcoin in the first transfer instruction into the second wallet without paying a miner's fee for the first transfer, receiving, over the network interface device, a second transfer instruction for an amount of bitcoin from the first wallet and a bitcoin address associated with a second node of the Bitcoin network, and in response to the second transfer instruction, recording a transfer in the first wallet for the amount of bitcoin in the second transfer instruction out of the first wallet, broadcasting a message to the Bitcoin network, including to the second node, to record a transfer associated with the bitcoin address

associated with the second node, for the amount of bitcoin in the second transfer instruction, and paying a miner's fee for the second transfer.

21. The host computer system of claim 20, wherein the set of instructions includes:

a login module that stores login details for the first wallet, receives login credentials for the first wallet from a first user device, verifies whether the login credentials match the login details for the first wallet, if the login credentials match the login details then logs the first user device into the first wallet, and if the first user device is logged into the wallet, permits the transfers based on the first transfer instruction and the second transfer instruction by a user of the first user device.

22. The host computer system of claim 21, wherein the set of instructions further includes:

a website receiving a user interface request from the first user device; and
a user interface of the website that is transmitted in response to the user interface request from the first user device, the user interface having at least one field for entering the login credentials and a field for selectably entering an identifier of the second wallet or bitcoin address associated with the second node.

23. The host computer system of claim 22, wherein the user interface includes a field for entering of the amount of bitcoin that is being transferred.

24. The host computer system of claim 22, wherein the login module:

stores login details for the second wallet, receives login credentials for the second wallet from a second user device, verifies whether the login credentials for the second wallet match the login details for the second wallet, if the login credentials match the login details then logs the second user device into the second wallet, and if the second user device is logged into the wallet, displays the amount of bitcoin being transferred based on the first transfer instruction.

25. The host computer system of claim 24, wherein the wallet management module determines whether a block chain verification notice has been received from the Bitcoin network indicating that the transfer based on the second transfer instruction has been verified, and records a notification in the first wallet that the transfer based on the second transfer instruction has been verified.

26. The host computer system of claim 25, wherein the wallet management module records a notification in the first wallet that the transfer based on the first transfer instruction has been processed without determining whether a block chain verification notice has been received.

27. The host computer system of claim 26, wherein the transfer based on the first transfer instruction is not broadcast to the Bitcoin network.

28. A method of transacting bitcoin comprising:
establishing, by a processor of a first host computer system at a first node of the

Bitcoin network, first and second wallets in a data store connected to the processor;
storing, by the processor, a value representative of an amount of bitcoin held by the first wallet;

receiving, by the processor, a first transfer instruction for an amount of bitcoin from the first wallet and an identifier of the second wallet;

in response to the first transfer instruction, by the processor, recording a transfer in the first wallet for the amount of bitcoin in the first transfer instruction out of the first wallet and a transfer in the second wallet, identified by the identifier of the second wallet, for the amount of bitcoin in the first transfer instruction into the second wallet without paying a miner's fee for the first transfer;

receiving, by the processor, a second transfer instruction for an amount of bitcoin from the first wallet and a bitcoin address associated with a second node of the bitcoin network;

in response to the second transfer instruction, by the processor, recording a transfer in the first wallet for the amount of bitcoin in the second transfer instruction out of the first wallet, broadcasting a message to the Bitcoin network, including to the second node, to record a transfer associated with the bitcoin address associated with the second node, for the amount of bitcoin in the second transfer instruction; and

paying, by the processor, a miner's fee for the second transfer.

29. The method of claim 28, further comprising:

storing, by the processor, login details for the first wallet;

receiving, by the processor, login credentials for the first wallet from a first user

device;

verifying, by the processor, whether the login credentials match the login details for the first wallet;

if the login credentials match the login details then, by the processor, logging the first user device into the first wallet; and

if the first user device is logged into the wallet, permitting, by the processor, the transfers based on the first transfer instruction and the second transfer instruction by a user of the first user device.

30. The method of claim 29, further comprising:

receiving, by the processor, a user interface request at a website from the first user device; and

transmitting, by the processor in response to the user interface request from the first user device, a user interface of the website to the first user device, the user interface having at least one field for entering the login credentials and a field for selectably entering an identifier of the second wallet or the bitcoin address associated with the second node.

31. The method of claim 30, wherein the user interface further include a field for entering of the amount of bitcoin that is being transferred.

32. The method of claim 30, further comprising:

storing, by the processor, login details for the second wallet;

receiving, by the processor, login credentials for the second wallet from a second

user device;

verifying, by the processor, whether the login credentials match the login details for the second wallet;

if the login credentials for the second wallet match the login details then, by the processor, logging the second user device into the second wallet; and

if the second user device is logged into the wallet, displaying, by the processor, the amount of bitcoin being transferred based on the first transfer instruction.

33. The method of claim 32, further comprising:

determining, by the processor, whether a block chain verification notice has been received from the Bitcoin network indicating that the transfer based on the second transfer instruction has been verified; and

recording, by the processor, a notification in the first wallet that the transfer based on the second transfer instruction has been verified.

34. The method of claim 33, further comprising:

recording a notification in the first wallet that the transfer based on the first transfer instruction has been processed without determining whether a block chain verification notice has been received.

35. The method of claim 34, wherein the transfer based on the first transfer instruction is not broadcast to the Bitcoin network.

36. A non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor of a first host computer system at a first node of the Bitcoin network to carry out a method of transacting bitcoin comprising:

establishing, by the processor, first and second wallets in a data store connected to the processor;

storing, by the processor, a value representative of an amount of bitcoin held by the first wallet;

receiving, by the processor, a first transfer instruction for an amount of bitcoin from the first wallet and an identifier of the second wallet;

in response to the first transfer instruction, by the processor, recording a transfer in the first wallet for the amount of bitcoin in the first transfer instruction out of the first wallet and a transfer in the second wallet, identified by the identifier of the second wallet, for the amount of bitcoin in the first transfer instruction into the second wallet without paying a miner's fee for the first transfer;

receiving, by the processor, a second transfer instruction for an amount of bitcoin from the first wallet and a bitcoin address associated with a second node of the bitcoin network;

in response to the second transfer instruction, by the processor, recording a transfer in the first wallet for the amount of bitcoin in the second transfer instruction out of the first wallet, broadcasting a message to the Bitcoin network, including to the second node, to record a transfer associated with the bitcoin address associated with the second node, for the amount of bitcoin in the second transfer instruction; and

paying, by the processor, a miner's fee for the second transfer.

BITCOIN PRIVATE KEY SPLITTING FOR COLD STORAGE

Inventors: Julian Langschaedel, Brian D. Armstrong and Fred E. Ehram

37. A host computer system for transacting bitcoin comprising:
- a processor;
 - a computer readable medium connected to the processor;
 - a local storage on the computer readable medium; and
 - a set of instruction on the computer readable medium that are executable by the processor, including:
 - a register;
 - a Bitcoin address and an associated private key and value stored in the register;
 - a local controller transferring a private key for a Bitcoin address of a vault, to a local storage connected to a processor and transferring the value of the Bitcoin address in the register to the vault;
 - a splitter that splits the private key of the Bitcoin address of the vault into a plurality of codes;
 - an offline distribution module distributing the codes to remote distributed storage locations, removing the private key of the Bitcoin address of the vault from the local storage, and removing the private key for the Bitcoin address of the register from the Bitcoin address of the register;
 - at least one restoration interface receiving at least some of the codes into which the private key for Bitcoin address of the vault has been split; and

an assembler that assembles the codes that have been received into the private key of the Bitcoin address of the vault, the local controller restoring the private key of the Bitcoin address of the vault from the local storage, and restoring the value for the Bitcoin address in the register from the vault.

38. The host computer system 37, wherein the value is transferred from the register to the vault after the codes have been distributed.

39. The host computer system 37, further comprising:
a wallet establishment module establishing a plurality of wallets in the local storage, the local controller storing at least one Bitcoin address for a value in association with each wallet, the local controller selecting at least a subset of the Bitcoin addresses in all the wallets, and storing the values of the subset of Bitcoin addresses to the vault.

40. The host computer system 37, further comprising:
an encryption algorithm encrypting each code before being distributed; and
a decryption algorithm decrypting the code after receiving the code.

41. The host computer system 37, wherein the number of codes that are distributed is more than the number of codes that are received before assembling the private key of the Bitcoin address.

42. The host computer system 41, wherein a minimum number of codes is required before the private key of the Bitcoin address can be assembled.

43. The host computer system 37, wherein the Bitcoin address for the register is a first Bitcoin address for the register, the codes are first codes, and the vault is a first vault, wherein the local controller transfers a private key for a second Bitcoin address of a second vault to the local storage connected to the processor, transfers the value of the second Bitcoin address in the register to the second vault, splits the private key for the Bitcoin address of the second vault into a plurality of second codes, the offline distribution module distributing the second codes to remote distributed storage locations, and the local controller removing the private key of the Bitcoin address of the second vault from the local storage, removing the private key for the second Bitcoin address of the register from the Bitcoin address of the register, the restoration interface receives at least some of the second codes into which the private key for Bitcoin address of the second vault has been split, the assembler assembles the second codes that have been received into the private key of the Bitcoin address of the second vault, and the local controller restores the private key of the second vault from the local storage, and restores the value for the second Bitcoin address in the register from the second vault.

44. A method of transacting bitcoin comprising:

transferring, by the processor, a private key of the Bitcoin address of a vault to a local storage connected to the processor;

splitting, by the processor, the private key of the Bitcoin address of the vault into a plurality of codes;

distributing the codes to remote distributed storage locations;

transferring, by the processor, a value of a Bitcoin address in a register to the vault;
receiving, by the processor, at least some of the codes into which the private key of the Bitcoin address of the vault has been split;

assembling, by the processor, the codes that have been received into the private key of the Bitcoin address of the vault;

restoring, by the processor, the private key of the Bitcoin address of the vault to the vault; and

restoring, by the processor, the value of the Bitcoin address in the register from the vault.

45. The method of claim 44, wherein the value is transferred from the register to the vault after the codes have been distributed.

46. The method of claim 44, further comprising:

establishing, by the processor, a plurality of wallets in the local register;

storing, by the processor, at least one Bitcoin address for a value in association with each wallet;

selecting, by the processor, at least a subset of the Bitcoin addresses in all the wallets; and

storing, by the processor, the values of the subset of Bitcoin addresses in the vault.

47. The method of claim 44, further comprising:

encrypting, by the processor, each code before being distributed; and

decrypting, by the processor, the code after receiving the code.

48. The method of claim 44, wherein the number of codes that are distributed is more than the number of codes that are received before assembling the private key.

49. The method of claim 48, wherein a minimum number of codes is required before the private key of the Bitcoin address can be assembled.

50. The method of claim 44, wherein the Bitcoin address for the register is a first Bitcoin address for the register, the codes are first codes, and the vault is a first vault, further comprising:

transferring, by the processor, a private key of the Bitcoin address of a second vault to a local storage connected to the processor;

splitting, by the processor, the private key of the Bitcoin address of the second vault into a plurality of second codes;

distributing the second codes to remote distributed storage locations;

transferring, by the processor, a value of a second Bitcoin address in the register to the vault;

receiving, by the processor, at least some of the second codes into which the private key for Bitcoin address of the second vault has been split;

assembling, by the processor, the second codes that have been received into the private key for Bitcoin address of the second vault;

restoring, by the processor, the private key of the second vault to the vault; and

restoring, by the processor, the value of the second Bitcoin address in the register from the second vault.

51. A non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor to carry out a method of transacting bitcoin comprising:

transferring, by the processor, a private key of a Bitcoin address of a vault to a local storage connected to the processor;

splitting, by the processor, the private key of the Bitcoin address of the vault into a plurality of codes;

distributing the codes to remote distributed storage locations;

transferring, by the processor, a value of a Bitcoin address in a register to the vault;

receiving, by the processor, at least some of the codes into which the private key of the Bitcoin address of the vault has been split;

assembling, by the processor, the codes that have been received into the private key of the Bitcoin address of the vault;

restoring, by the processor, the private key of the Bitcoin address of the vault to the vault; and

restoring, by the processor, the value of the Bitcoin address in the register from the vault.

HOT WALLET FOR HOLDING BITCOIN

Inventors: Julian Langschaedel, Brian D. Armstrong and Fred E. Ehram

52. A host computer system for transacting bitcoin comprising:
- a processor;
 - a network interface device connected to the processor;
 - a computer readable medium connected to the processor;
 - a local storage on the computer readable medium; and
 - a set of instructions on the computer readable medium that are executable by the processor, including:
 - a wallet;
 - a plurality of Bitcoin addresses stored in the wallet;
 - a first vault;
 - a local controller selecting a first transfer set of the Bitcoin addresses for cold storage in the first vault, transferring at least a portion of each of the Bitcoin addresses of the first transfer set to a first vault while keeping the portions a first transaction set in the register, and restoring at least the portion of the Bitcoin addresses of the first transfer set from the first vault to the wallet; and
 - a wallet management module transacting using the Bitcoin addresses of the first transacting set without permitting transacting with the Bitcoin addresses of the first transfer set due to the portions thereof being restored to the first vault, and transacting using the Bitcoin addresses of the first transfer set due to the portions thereof being restored from the first vault to the wallet.
53. The host computer system 52, wherein the local controller selects a transfer set of the Bitcoin addresses for cold storage in a second vault, and transfers at least a portion of each

of the Bitcoin addresses of the second transfer set to the second vault, and the wallet management module transacts using the Bitcoin addresses of the first transfer set without permitting transacting with the Bitcoin addresses of the second transfer set due to the portions thereof being transferred to the second vault.

54. The host computer system 52, wherein the portions of the second transfer set are transferred to the second vault before the portions of the first transfer set are restored from the vault.

55. The host computer system 53, wherein the local controller selects a third transfer set of the Bitcoin addresses for cold storage in a third vault, and transfers at least a portion of each of the Bitcoin addresses of the third transfer set to the third vault while keeping the portions a second transaction set in the register, and the wallet management module transacts using the Bitcoin addresses of the second transacting set without permitting transacting with the Bitcoin addresses of the third transfer set due to the portions thereof being transferred to the third vault.

56. The host computer system 52, wherein each Bitcoin address has a public key, a private key and a value, the portions being the respective values.

57. The host computer system 56, wherein the local controller stores a private key for the Bitcoin address of the vault in a local storage connected to a processor, further comprising:
a splitter that splits the private key of the Bitcoin address of the vault into a plurality

of codes;

an offline distribution module distributing the codes to remote distributed storage locations, removing the private key of the Bitcoin address of the vault from the local storage, and removing the private key for the Bitcoin address of the register from the Bitcoin address of the register;

at least one restoration interface receiving at least some of the codes into which the private key of the Bitcoin address of the vault has been split;

an assembler that assembles the codes that have been received into the private key of the Bitcoin address of the vault, the local controller restoring the private key of the Bitcoin address of the vault from the local storage and restoring the value for the Bitcoin address in the register from the vault.

58. A method of transacting bitcoin comprising:

storing, by a processor, a plurality of Bitcoin addresses in a wallet;

selecting, by the processor, a first transfer set of the Bitcoin addresses for cold storage in a first vault;

transferring, by the processor, at least a portion of each of the Bitcoin addresses of the first transfer set to the first vault while keeping the portions a first transaction set in the register;

transacting, by the processor, using the Bitcoin addresses of the first transacting set without permitting transacting with the Bitcoin addresses of the first transfer set due to the portions thereof being transferred to the first vault;

restoring, by the processor, the portion of the Bitcoin addresses of the first transfer

set from the first vault to the wallet; and

transacting, by the processor, using the Bitcoin addresses of the first transfer set due to the portions thereof being restored from the first vault to the wallet.

59. The method of claim 58, further comprising:

selecting, by the processor, a second transfer set of the Bitcoin addresses for cold storage in a second vault;

transferring, by the processor, at least a portion of each of the Bitcoin addresses of the second transfer set to the second vault while keeping the portions a second transaction set in the register; and

transacting, by the processor, using the Bitcoin addresses of the second transacting set without permitting transacting with the Bitcoin addresses of the second transfer set due to the portions thereof being transferred to the second vault.

60. The method of claim 59, wherein the portions of the second transfer set are transferred to the second vault before the portions of the first transfer set are restored from the vault.

61. The method of claim 60, further comprising:

selecting, by the processor, a third transfer set of the Bitcoin addresses for cold storage in a third vault;

transferring, by the processor, at least a portion of each of the Bitcoin addresses of the third transfer set to the third vault while keeping the portions a third transaction set in the

register; and

transacting, by the processor, using the Bitcoin addresses of the third transacting set without permitting transacting with the Bitcoin addresses of the third transfer set due to the portions thereof being transferred to the third vault.

62. The method of claim 58, wherein each Bitcoin address has a public key and a private key, the portions being the private keys.

63. A non-transitory computer-readable medium having stored thereon a set of instructions that are executable by a processor to carry out a method of transacting bitcoin comprising:

storing, by a processor, a plurality of Bitcoin addresses in a wallet;

selecting, by the processor, a first transfer set of the Bitcoin addresses for cold storage in a first vault;

transferring, by the processor, at least a portion of each of the Bitcoin addresses of the first transfer set to the first vault while keeping the portions a first transaction set in the register;

transacting, by the processor, using the Bitcoin addresses of the first transacting set without permitting transacting with the Bitcoin addresses of the first transfer set due to the portions thereof being transferred to the first vault;

restoring, by the processor, the portion of the Bitcoin addresses of the first transfer set from the first vault to the wallet; and

transacting, by the processor, using the Bitcoin addresses of the first transfer set due to the

portions thereof being restored from the first vault to the wallet.

ABSTRACT OF THE DISCLOSURE

A system and method for transaction bitcoin is described. Bitcoin can be sent to an email address. No miner's fee is paid by a host computer system. Hot wallet functionality is provided that transfers values of some Bitcoin addresses to a vault for purposes of security. A private key of a Bitcoin address of the vault is split and distributed to keep the vault secure.

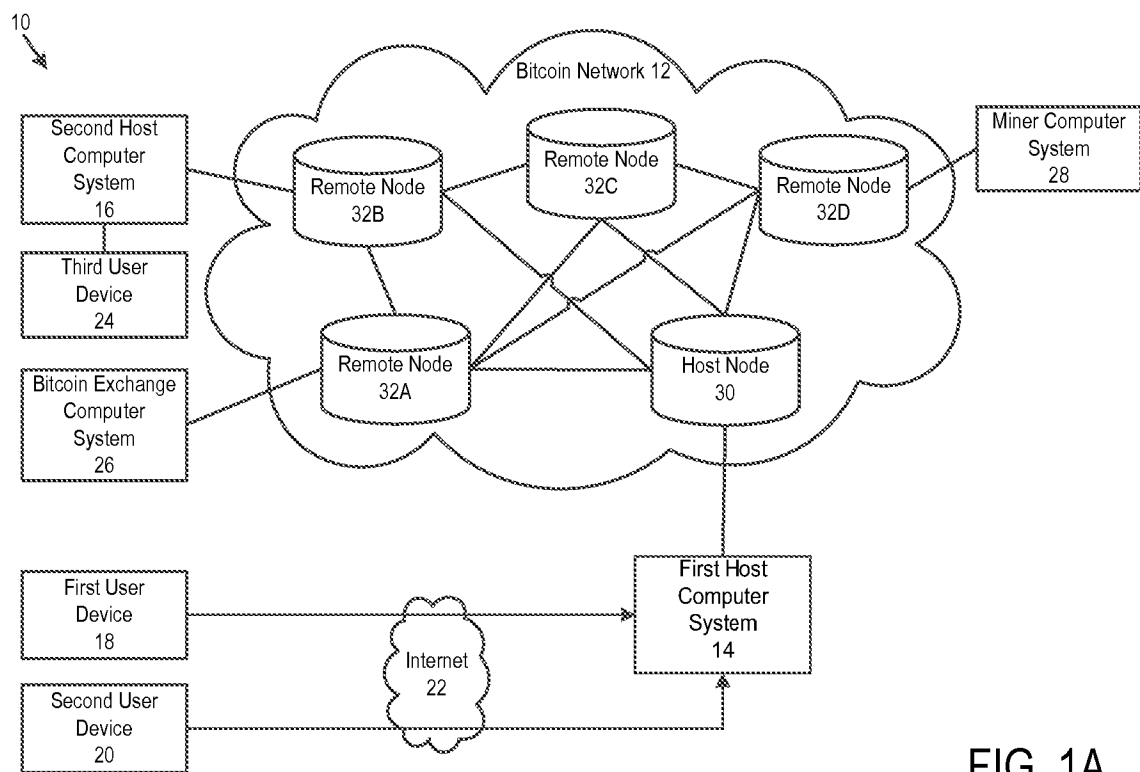


FIG. 1A

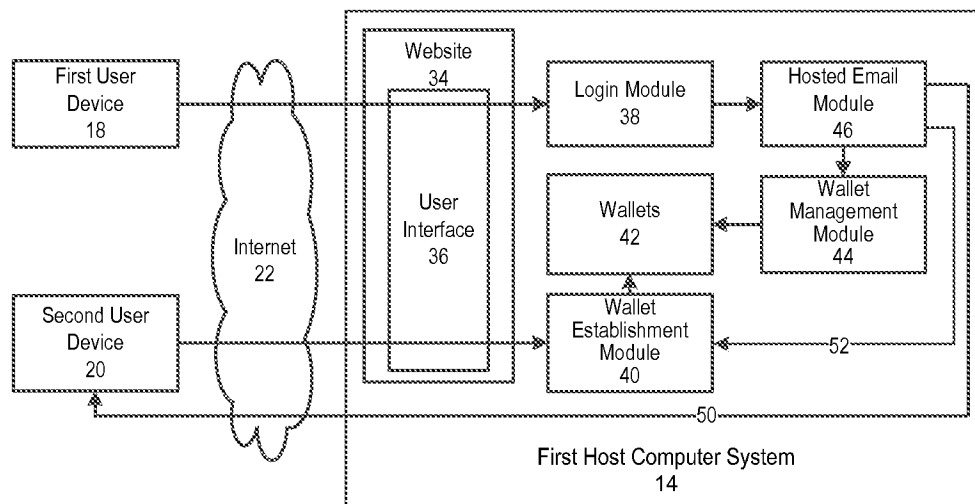


FIG. 1B

	First Host Computer System 14	
	Wallet A	
	Email address A; Login Details	
Transfer 1	Bitcoin address 1	
		From: First Host
		Amount in bitcoin
		Host Fee: x%
Transfer 2	Bitcoin address 2	
		From: Network address
		Amount in bitcoin
		Host Fee: 0 bitcoin

FIG. 2

	First Host Computer System 14			
	Wallet A		Wallet B	
	Email address A; Login Details		Email address B	
Transfer 1	Bitcoin address 1			
		From: First Host		
		Amount in bitcoin		
		Host Fee: x%		
Transfer 2	Bitcoin address 2			
		From: Network address		
		Amount in bitcoin		
		Host Fee: 0 bitcoin		
Transfer 3	Bitcoin address 2		Bitcoin address 3	
		To: Email address B		From: Wallet A
		Amount in bitcoin		Amount in bitcoin
		Miner's Fee = 0 bitcoin		
		Host Fee: 0 bitcoin		

FIG. 3

 coinbase

Hi Buyer01@domain.com

RepresentativeA just sent you **0.00189 BTC** (worth \$1 USD)
using Coinbase.

Attached message:

Have some bitcoin and get a Coinbase account!

Bitcoin is a new digital currency that is being used all over the world.

[Click here to sign in and claim this amount](#)

Kind regards,
The Coinbase Team

FIG. 4

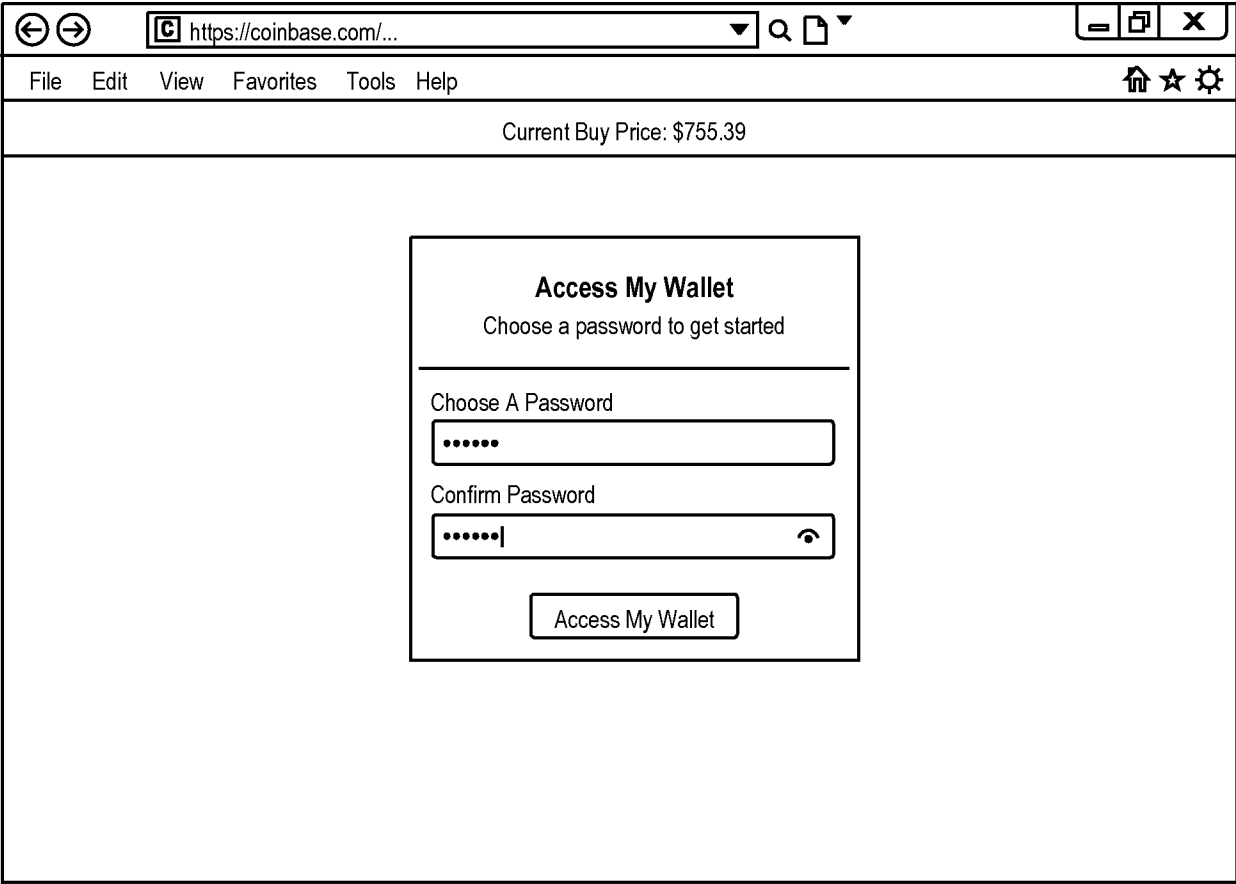


FIG. 5

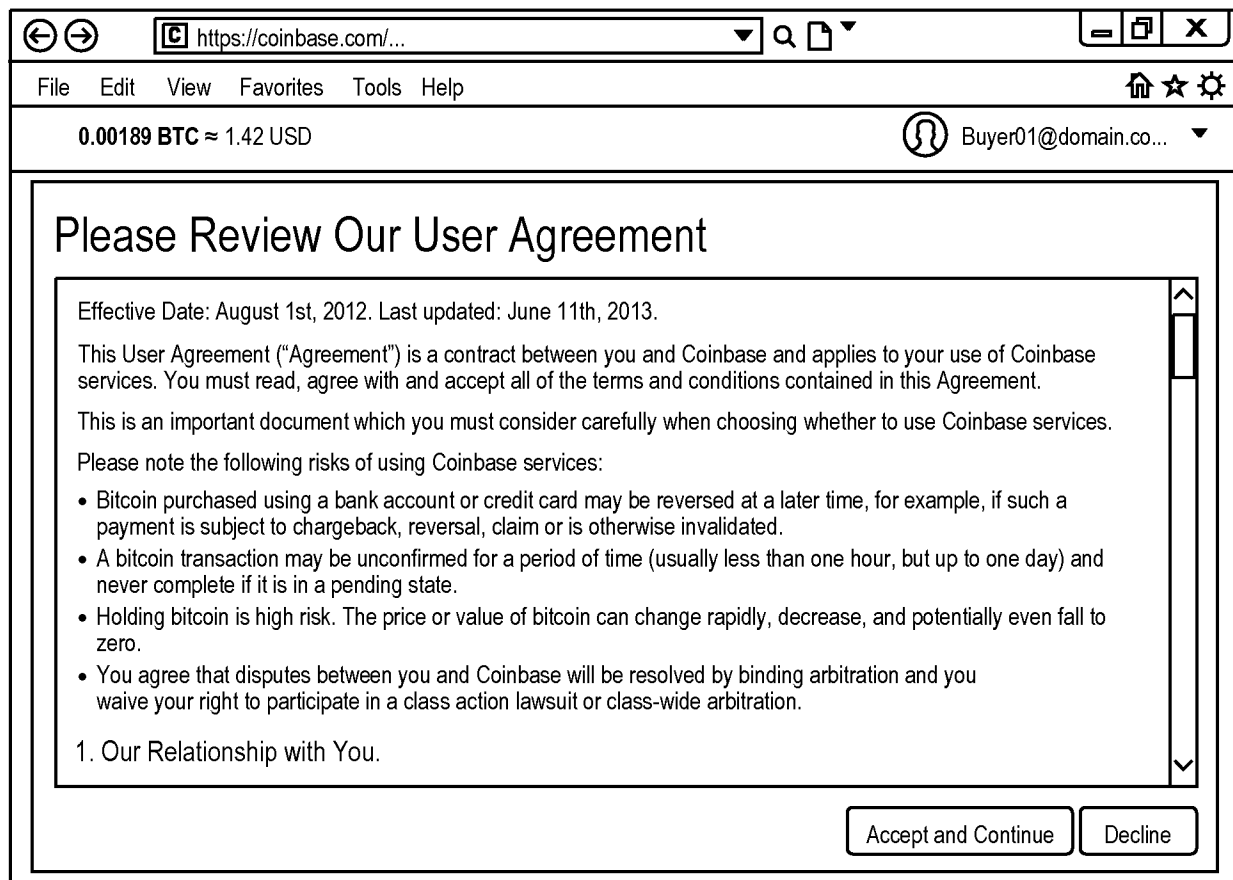


FIG. 6

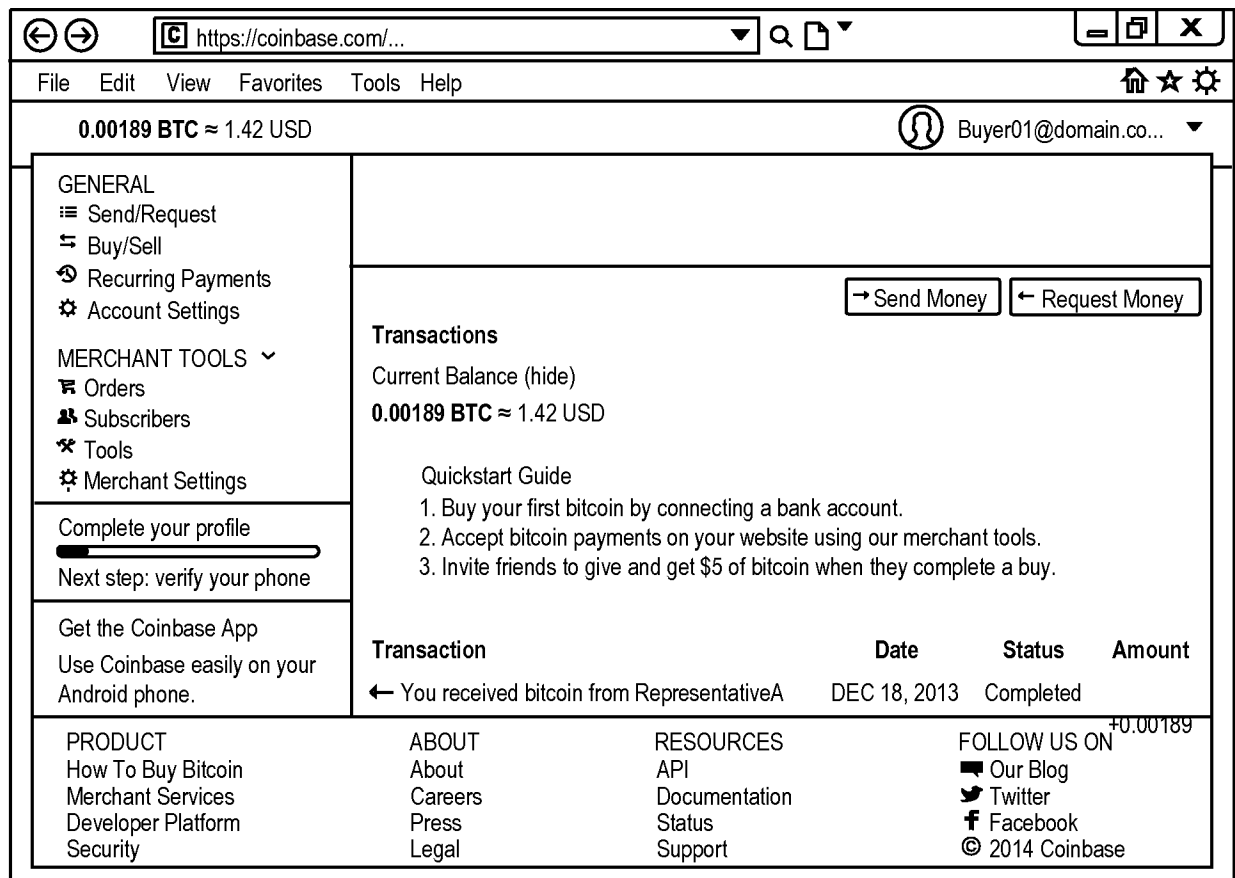


FIG. 7

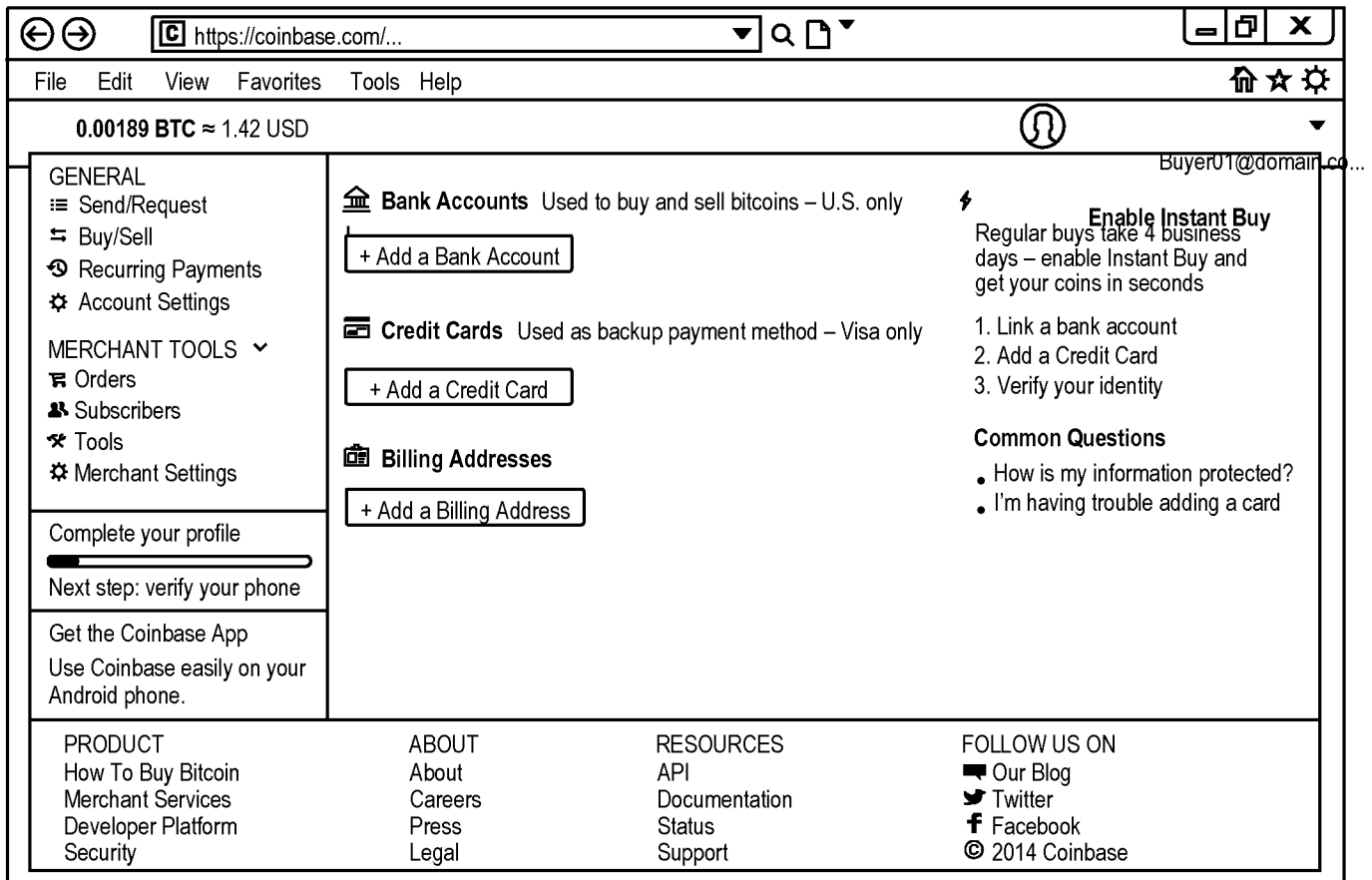


FIG. 8

[illegible]

FIG. 9

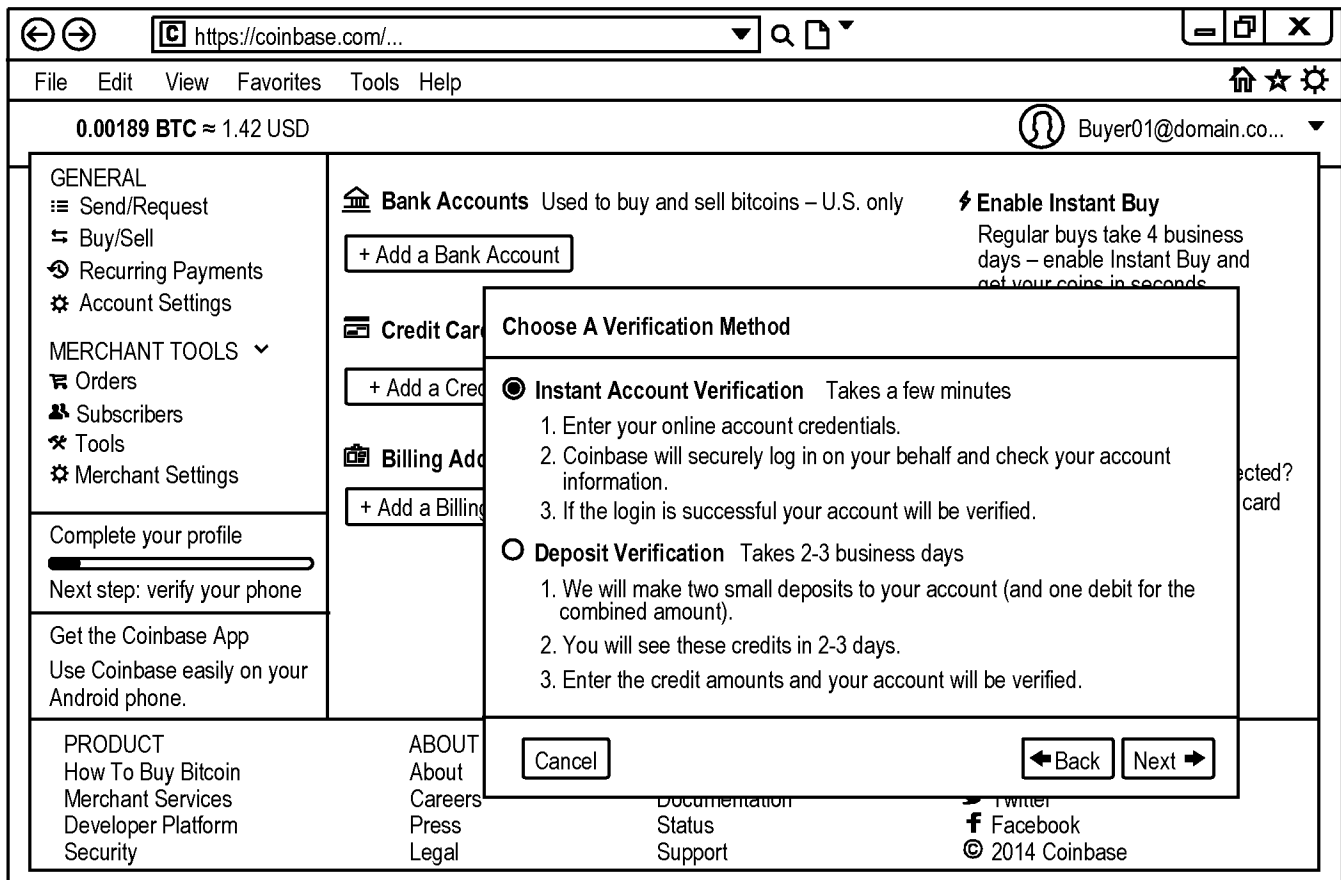


FIG. 10

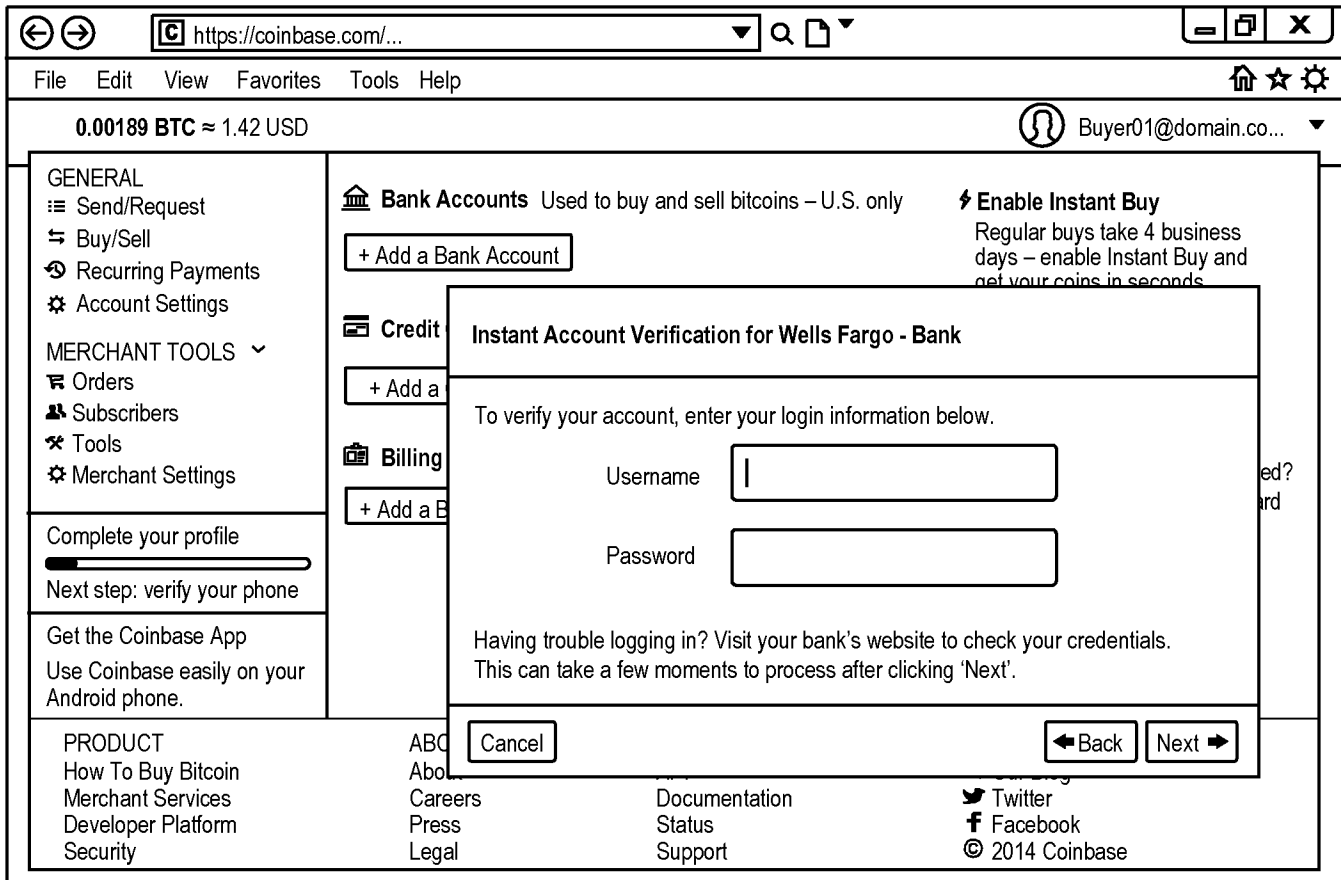


FIG. 11

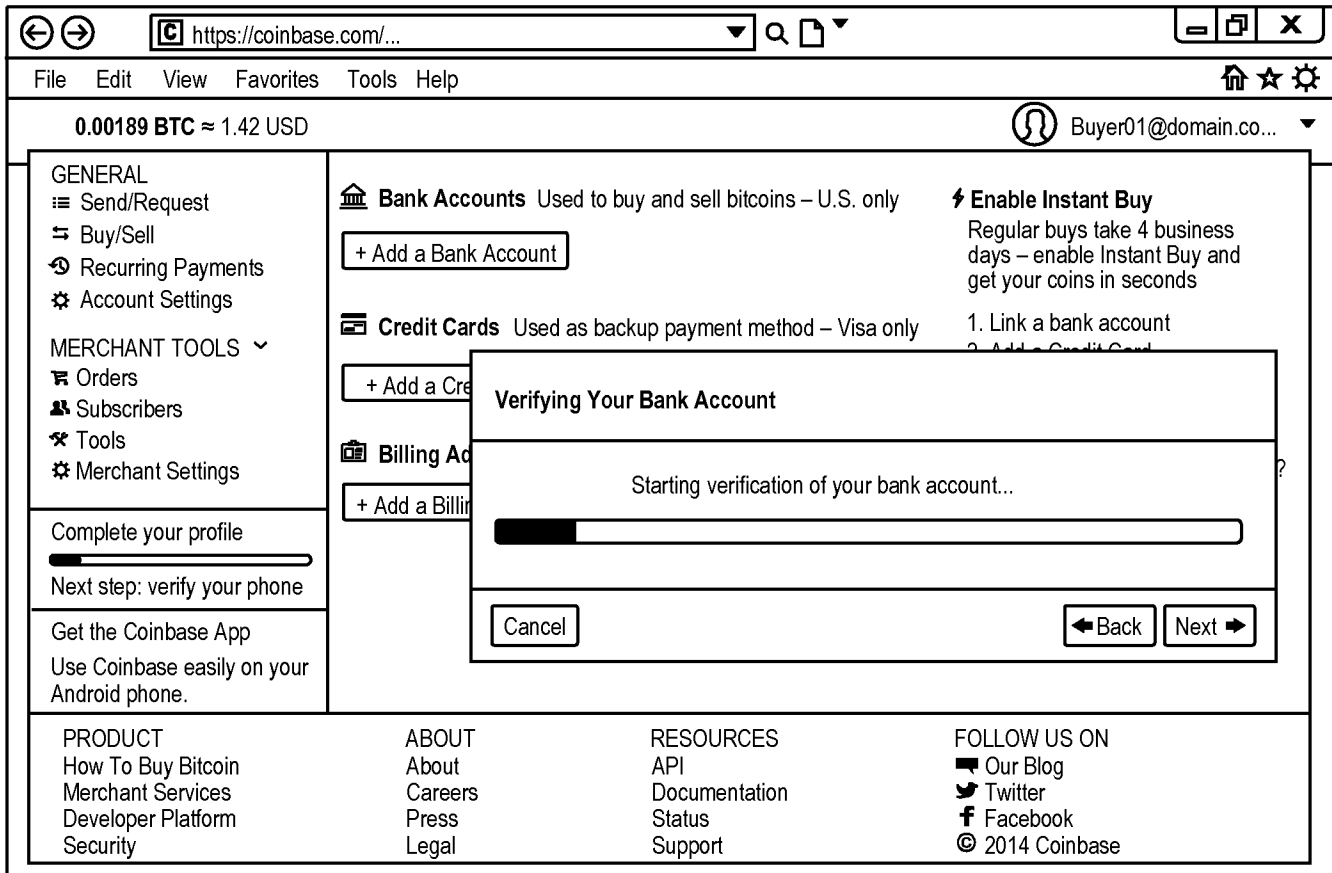


FIG. 12

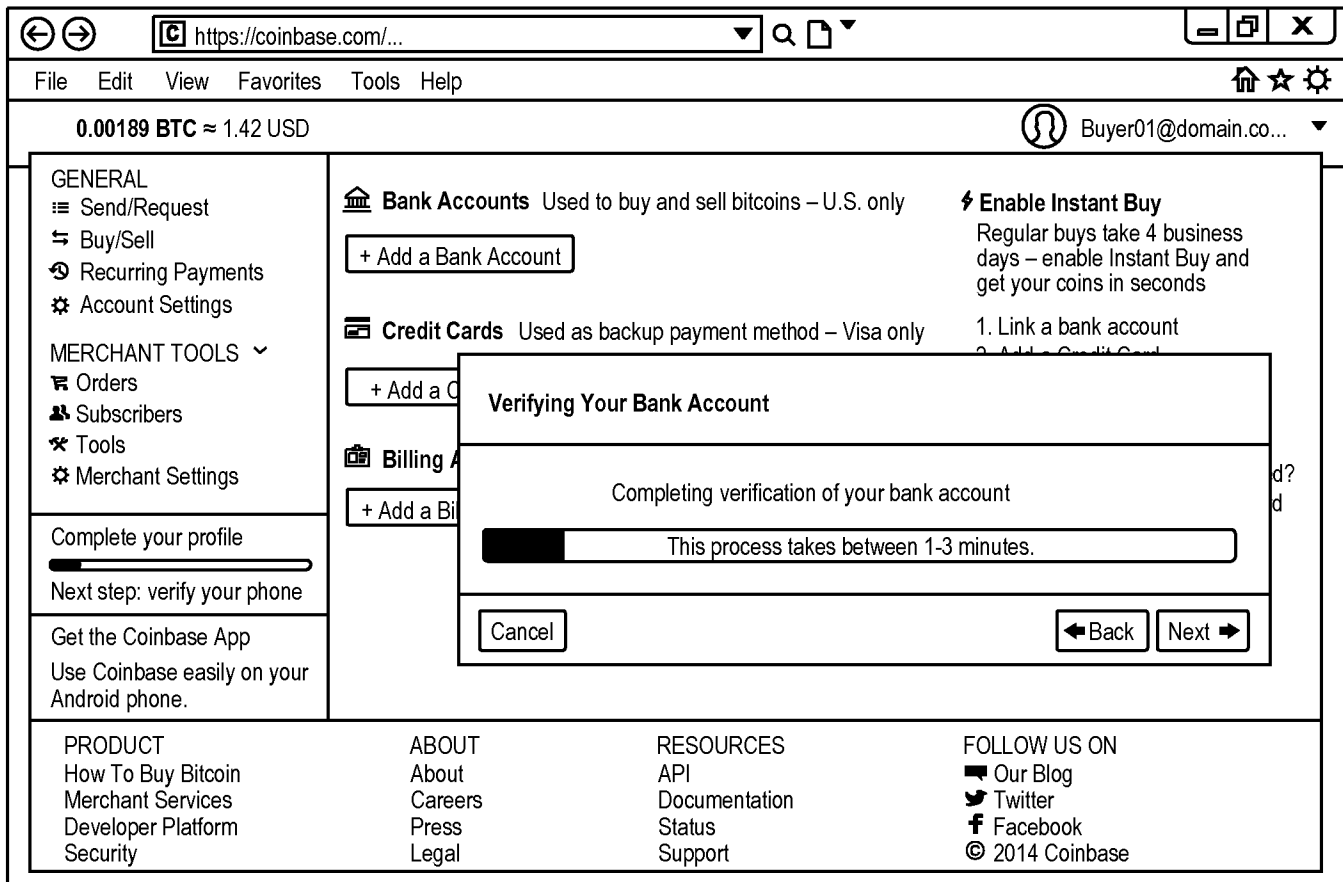


FIG. 13

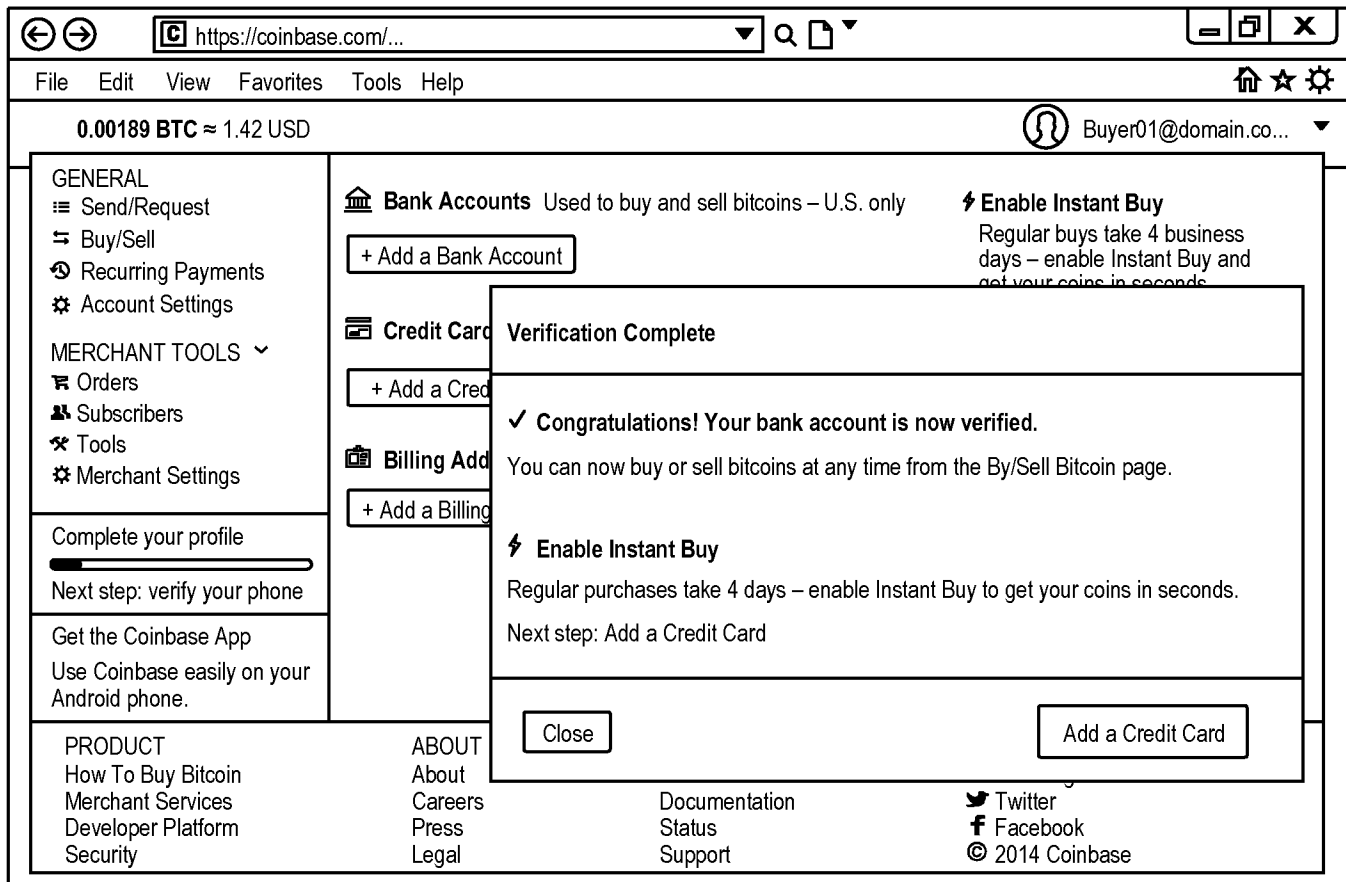


FIG. 14

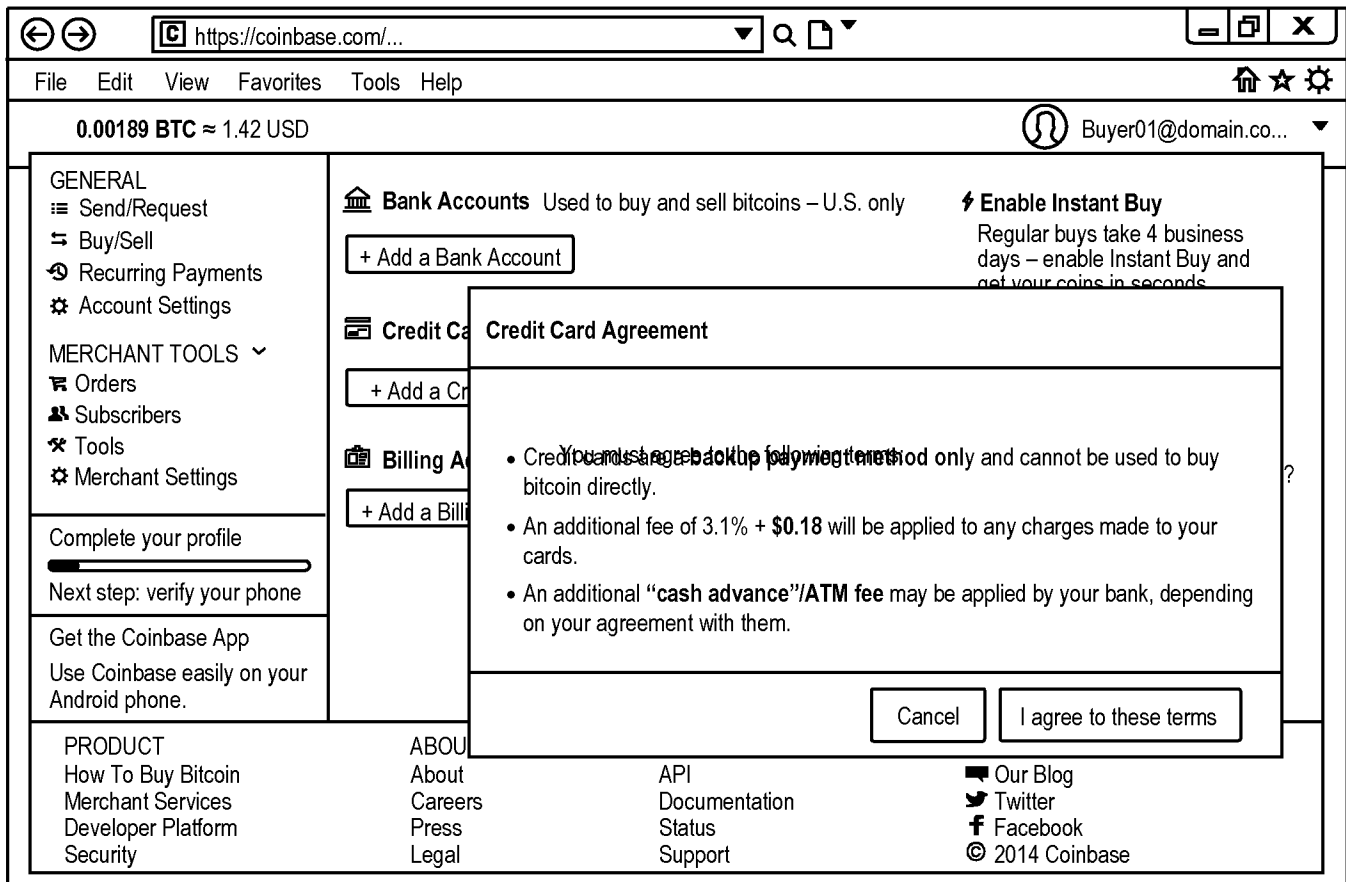


FIG. 15

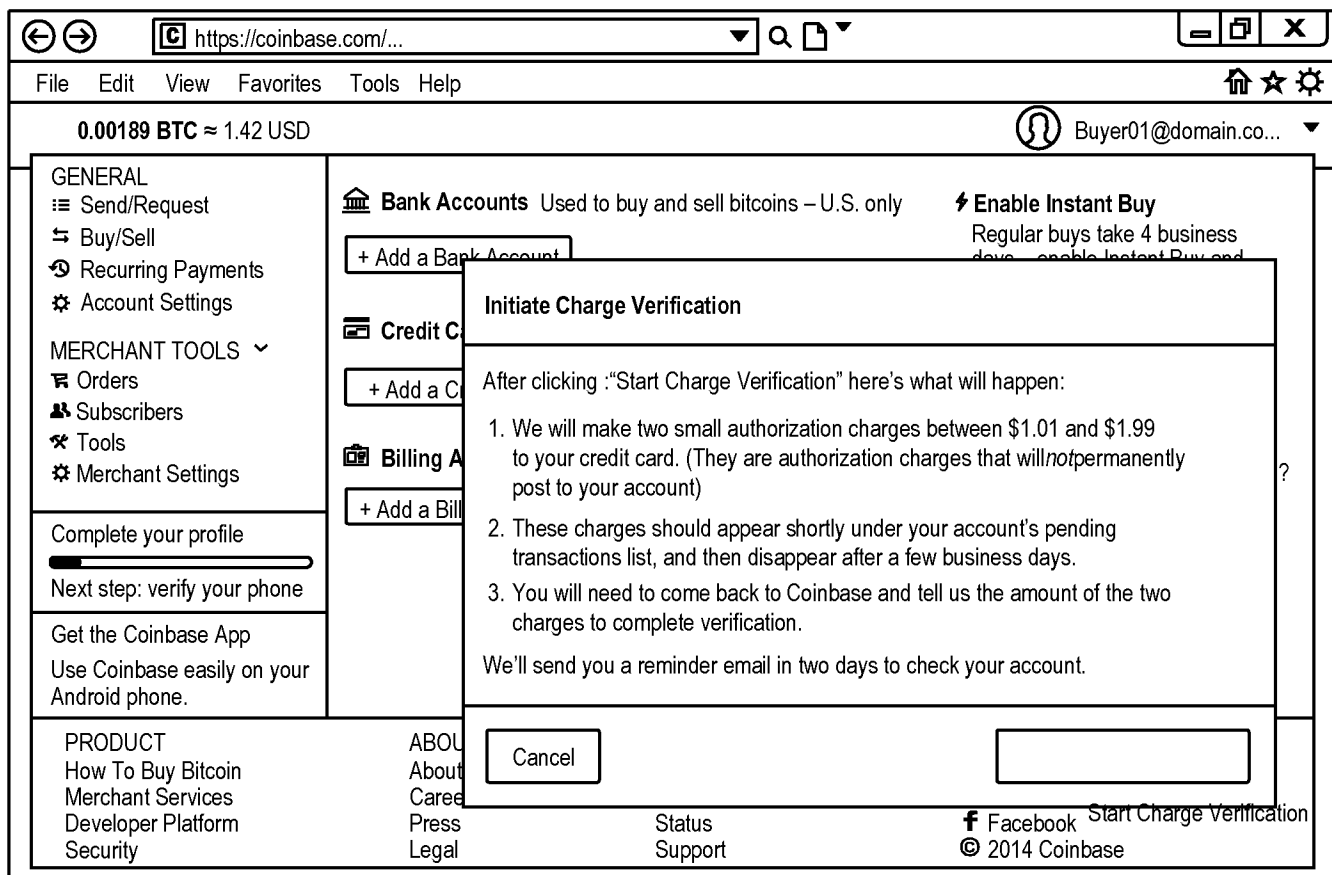


FIG. 18

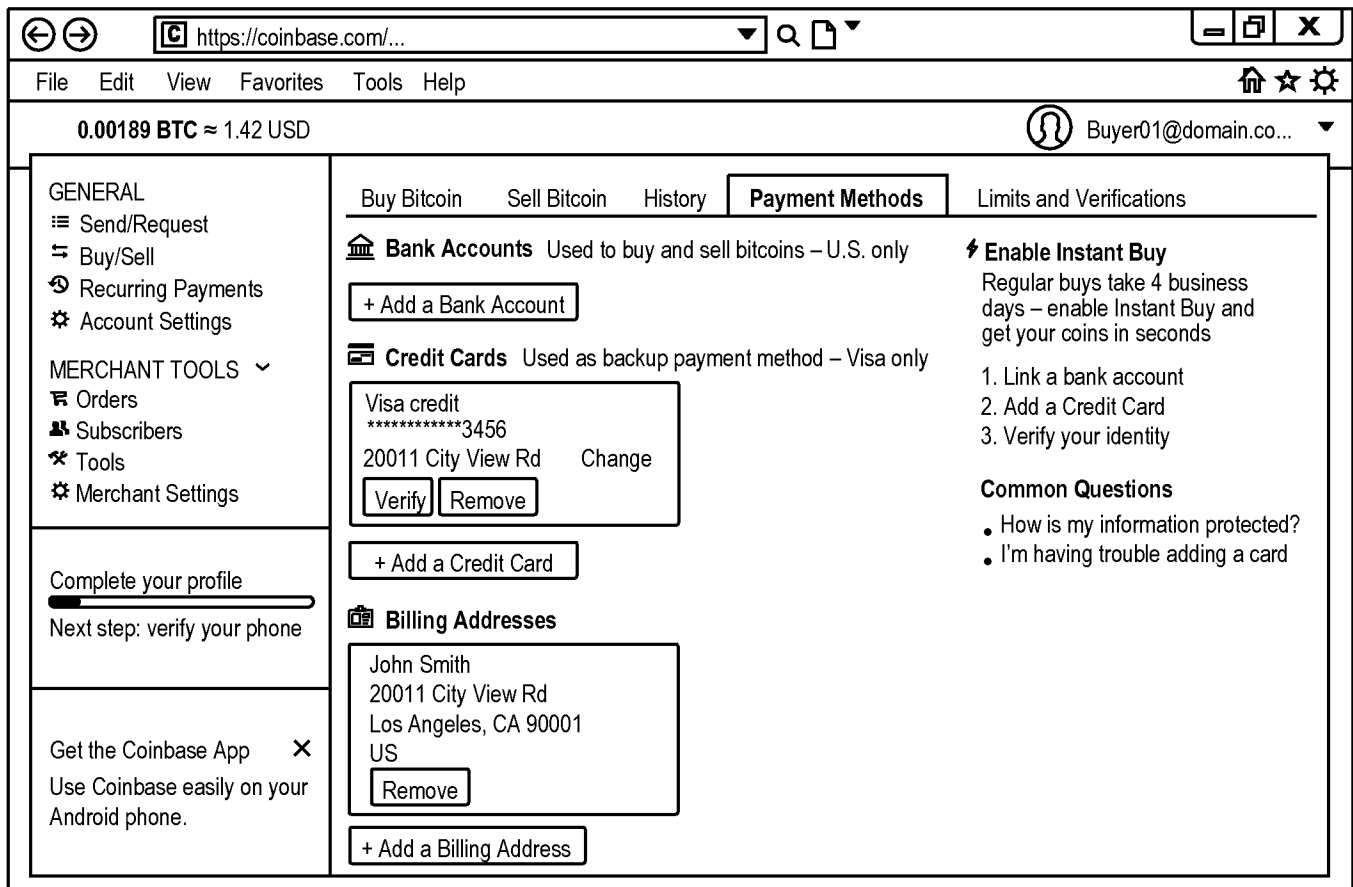


FIG. 19

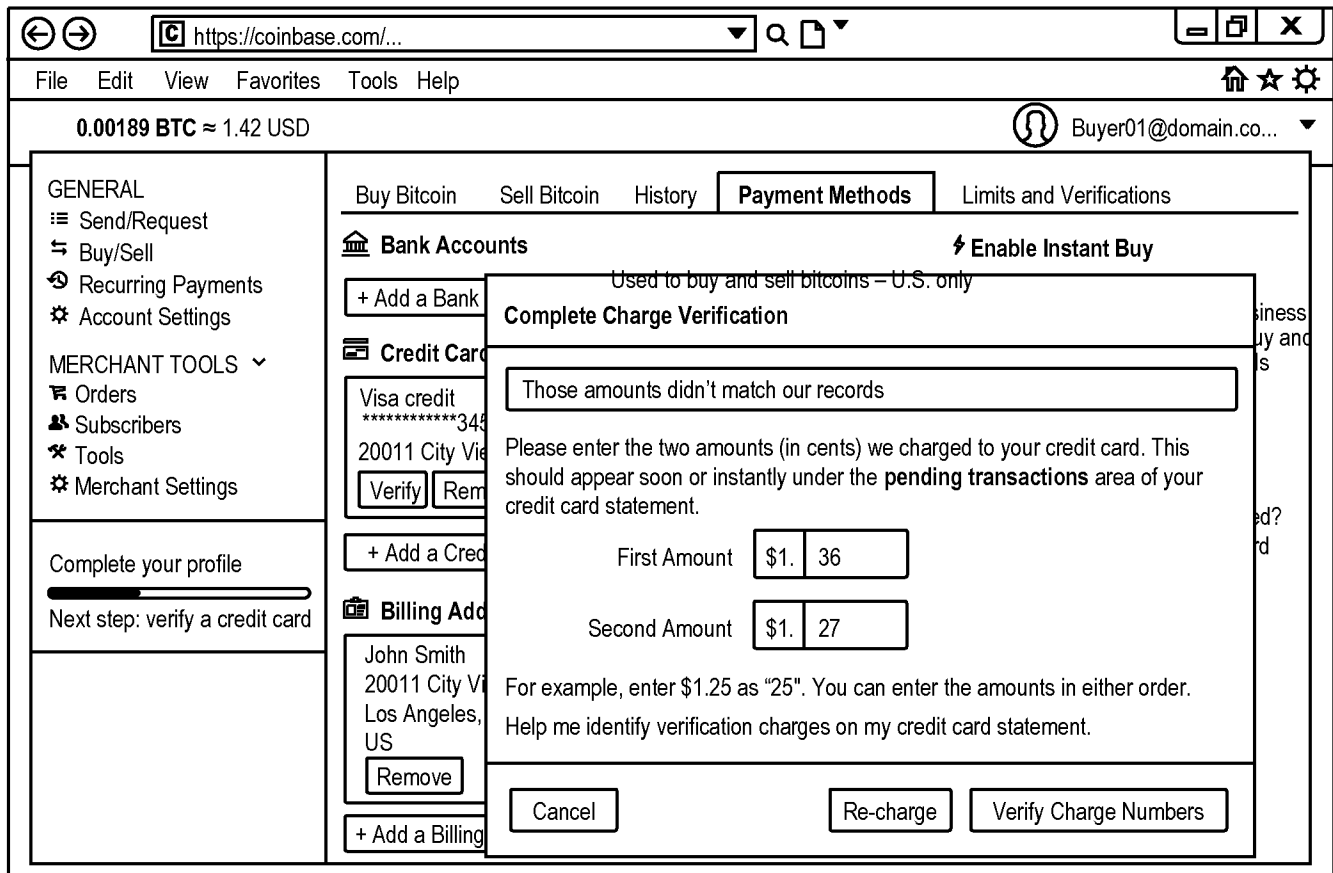


FIG. 20

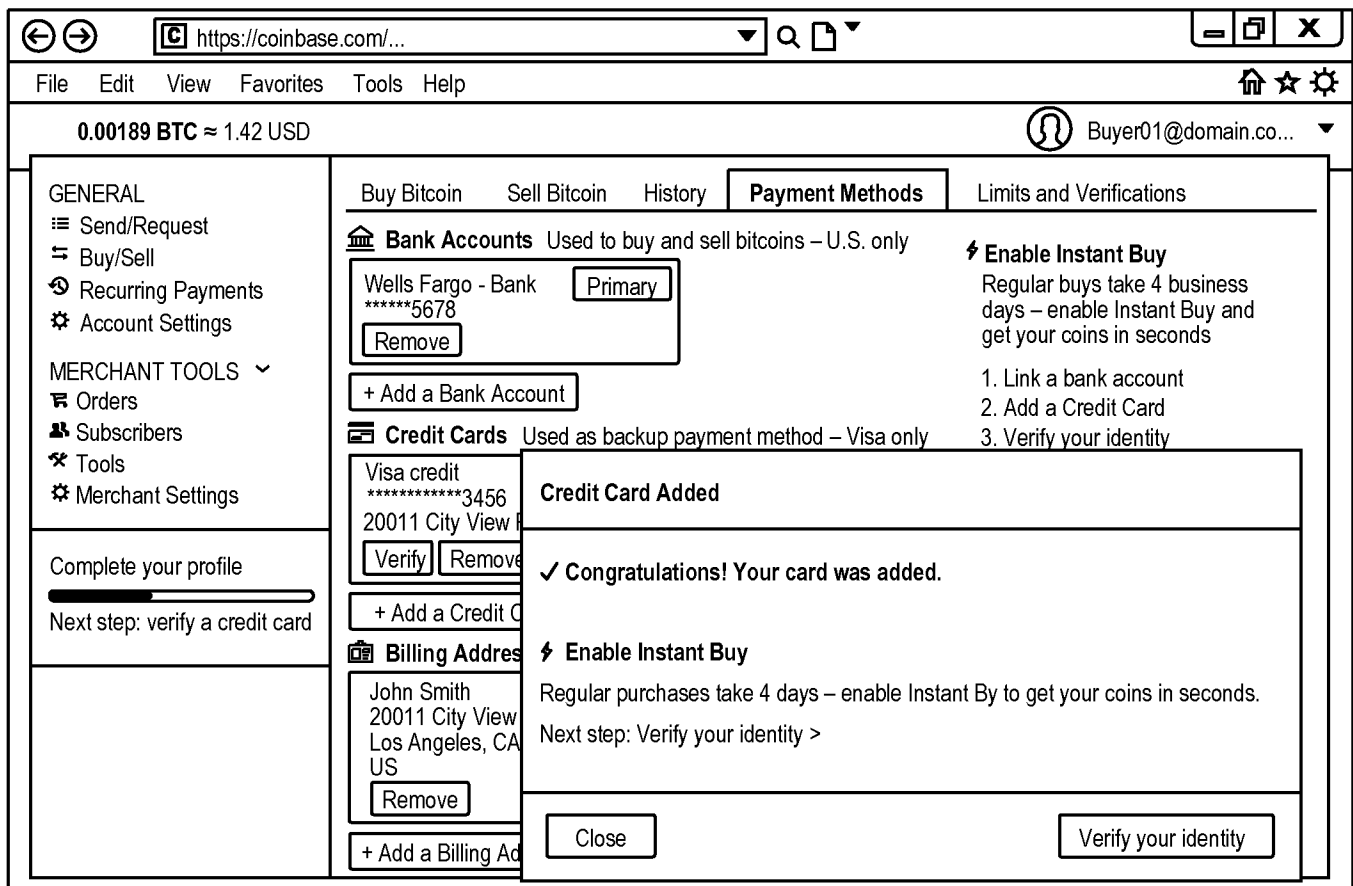


FIG. 21

https://coinbase.com/...

FileEditViewFavoritesToolsHelp

0.00189 BTC ≈ 1.42 USD

Buyer01@domain.co...

GENERAL

- Send/Request
- Buy/Sell
- Recurring Payments
- Account Settings

MERCHANT TOOLS

- Orders
- Subscribers
- Tools
- Merchant Settings

Complete your profile

Next step: verify your phone

Account SettingsReferralsBitcoin AddressesIntegrations

Account Settings

Name

Email

buyer01@domain.com

Local currency

United States, Dollar (USD)

Time zone

(GMT -08:00) Pacific Time (US)

Save Changes

Password

Change Password

Forgot Password?

Picture

Change Picture

Phone Numbers

adding a phone enables two-factor authentication on your account. read more

+ Verify A Phone

Notifications

Email me when:

☒ I send or receive bitcoin

☒ I buy or sell bitcoin

☒ I receive merchant orders

☒ There are recommended actions for my account

Save Changes

Reports

Export my

transaction history

and email it to

buyer01@doman.com

Export

FIG. 22

https://coinbase.com/...

FileEditViewFavoritesToolsHelp

0.00189 BTC ≈ 1.42 USD

Buyer01@domain.co...

Account updated!

GENERAL

Send/Request

Buy/Sell

Recurring Payments

Account Settings

MERCHANT TOOLS

Orders

Subscribers

Tools

Merchant Settings

Complete your profile

Next step: verify your phone

Account SettingsReferralsBitcoin AddressesIntegrations

Account Settings

Name

John Smith

Email

buyer01@domain.com

Local currency

United States, Dollar (USD)

Time zone

(GMT -08:00) Pacific Time (US)

Save Changes

Phone Numbers

adding a phone enables two-factor authentication on your account. read more

+ Verify A Phone

Notifications

Email me when:

☒ I send or receive bitcoin

☒ I buy or sell bitcoin

☒ I receive merchant orders

☒ There are recommended actions for my account

Save Changes

Reports

Export my

transaction history

and email it to

buyer01@doman.com

Export

FIG. 23

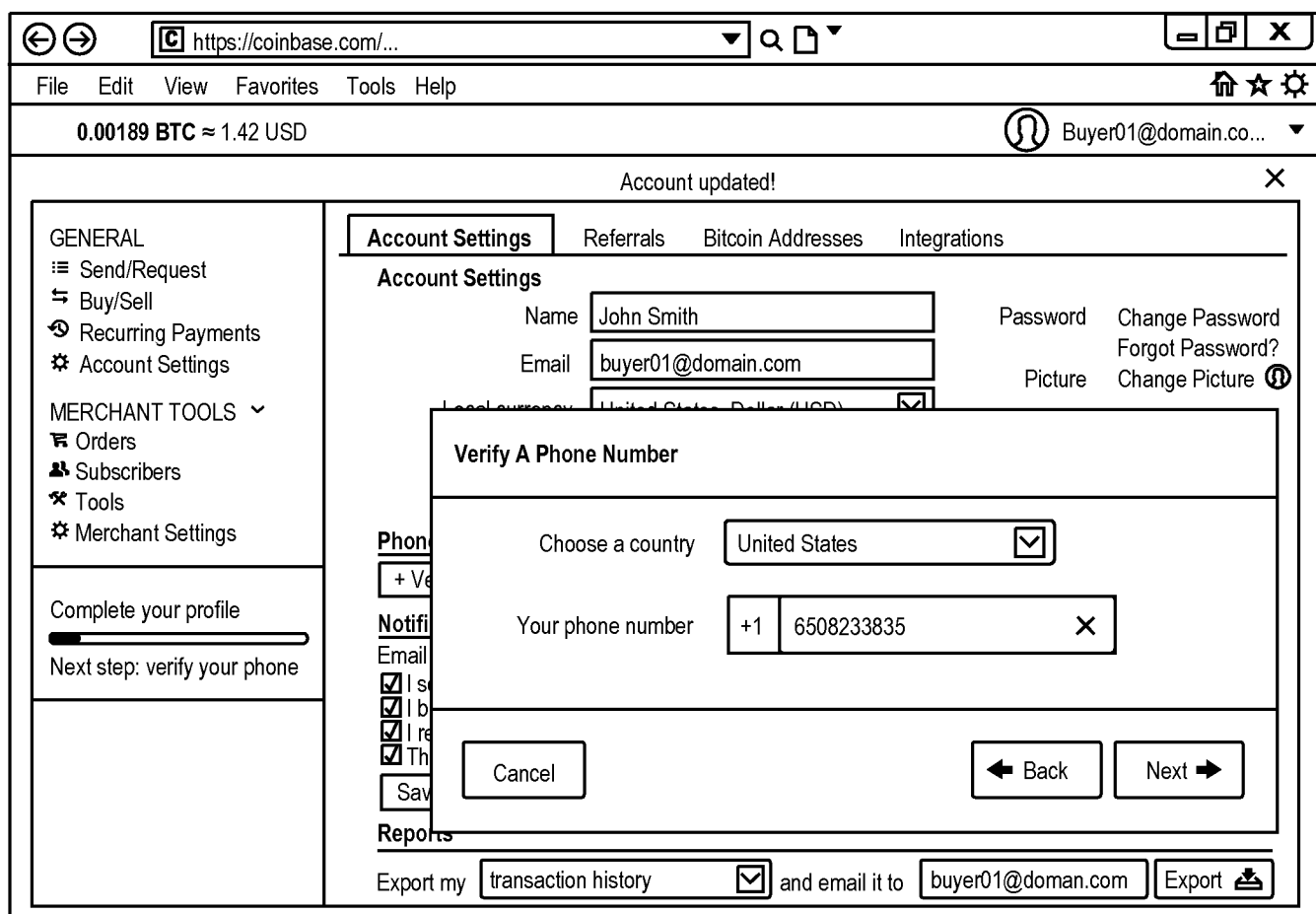


FIG. 25

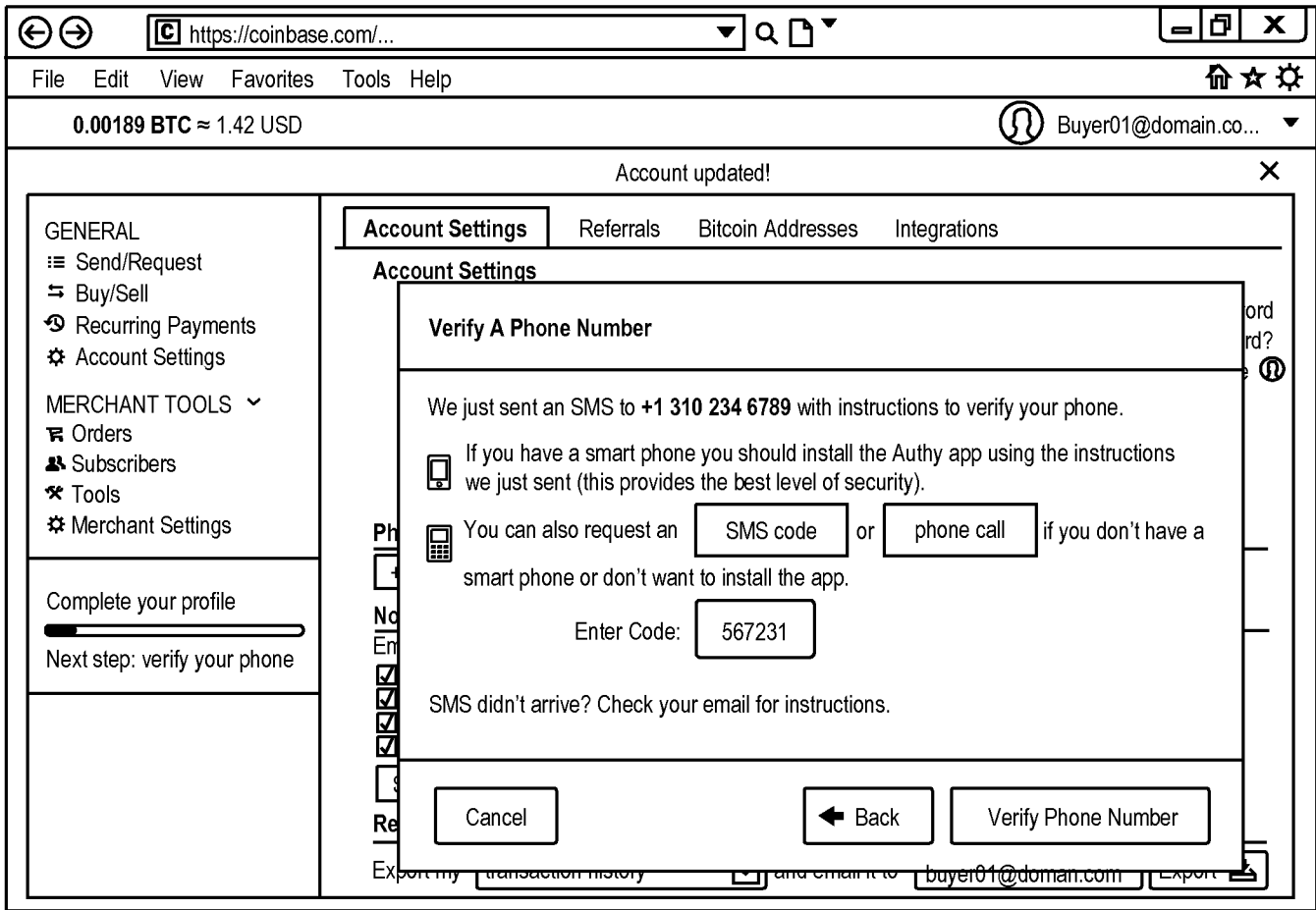


FIG. 26

https://coinbase.com/...

FileEditViewFavoritesToolsHelp

0.00189 BTC ≈ 1.42 USD

Buyer01@domain.co...

Account updated!

GENERAL

- Send/Request
- Buy/Sell
- Recurring Payments
- Account Settings

MERCHANT TOOLS

- Orders
- Subscribers
- Tools
- Merchant Settings

Complete your profile

Next step: verify your phone

Account SettingsReferralsBitcoin AddressesIntegrations

Account Settings

Name

John Smith

Email

buyer01@domain.com

Local currency

United States, Dollar (USD)

Time zone

(GMT -08:00) Pacific Time (US)

Save Changes

Password

Change Password

Forgot Password?

Picture

Change Picture

Phone Numbers

adding a phone enables two-factor authentication on your account. read more

+1 310 234 6789

VERIFIED

PRIMARY PHONE

Delete

You can also Google Authenticator and SMS access

Notifications

Email me when:

☒ I send or receive bitcoin

☒ I buy or sell bitcoin

☒ I receive merchant orders

☒ There are recommended actions for my account

Save Changes

Reports

Export my

transaction history

and email it to

buyer01@doman.com

Export

FIG. 27

https://coinbase.com/...

FileEditViewFavoritesToolsHelp

0.00189 BTC ≈ 1.42 USD

Buyer01@domain.co...

GENERAL

☰ Send/Request

➡ Buy/Sell

🔄 Recurring Payments

⚙ Account Settings

MERCHANT TOOLS ▾

📦 Orders

👤 Subscribers

🔧 Tools

⚙ Merchant Settings

Complete your profile

Next step: verify your identity

PRODUCT

How To Buy Bitcoin

Merchant Services

Developer Platform

Security

ID Verification Step 2: Questions

Information pulled from public records

Where was your social security number issued?

☐ Oregon

☒ California

☐ Arkansas

☐ None of the above

☐ Kentucky

You have 4 minutes to complete

With which name are you associated?

☐ ARDONNE

☐ MARQUIS

☐ HANLEY

☒ None of the above

☐ ILFORD

In which city is LEIGH AVE?

☐ BETHESDA

☐ SACRAMENTO

☐ HIGHLAND PARK

☐ None of the above

☒ LOS ANGELES

How long have you been associated with the property at 20011 City View Rd?

☐ Less than 2 years

☒ 4 - 5 years

☐ 2 - 3 years

☐ Over 5 years

☐ 3 - 4 years

☐ None of the above

Submit

FIG. 29

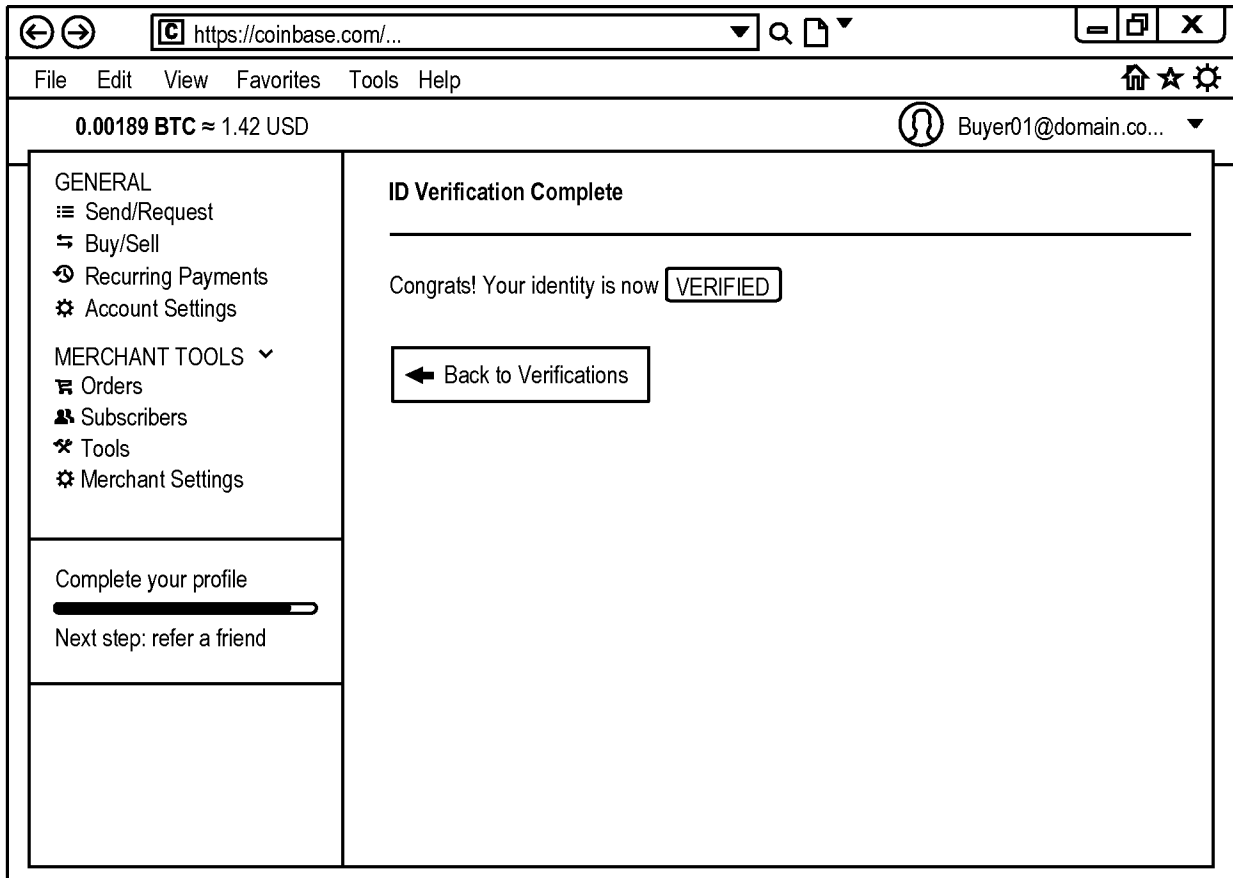


FIG. 30

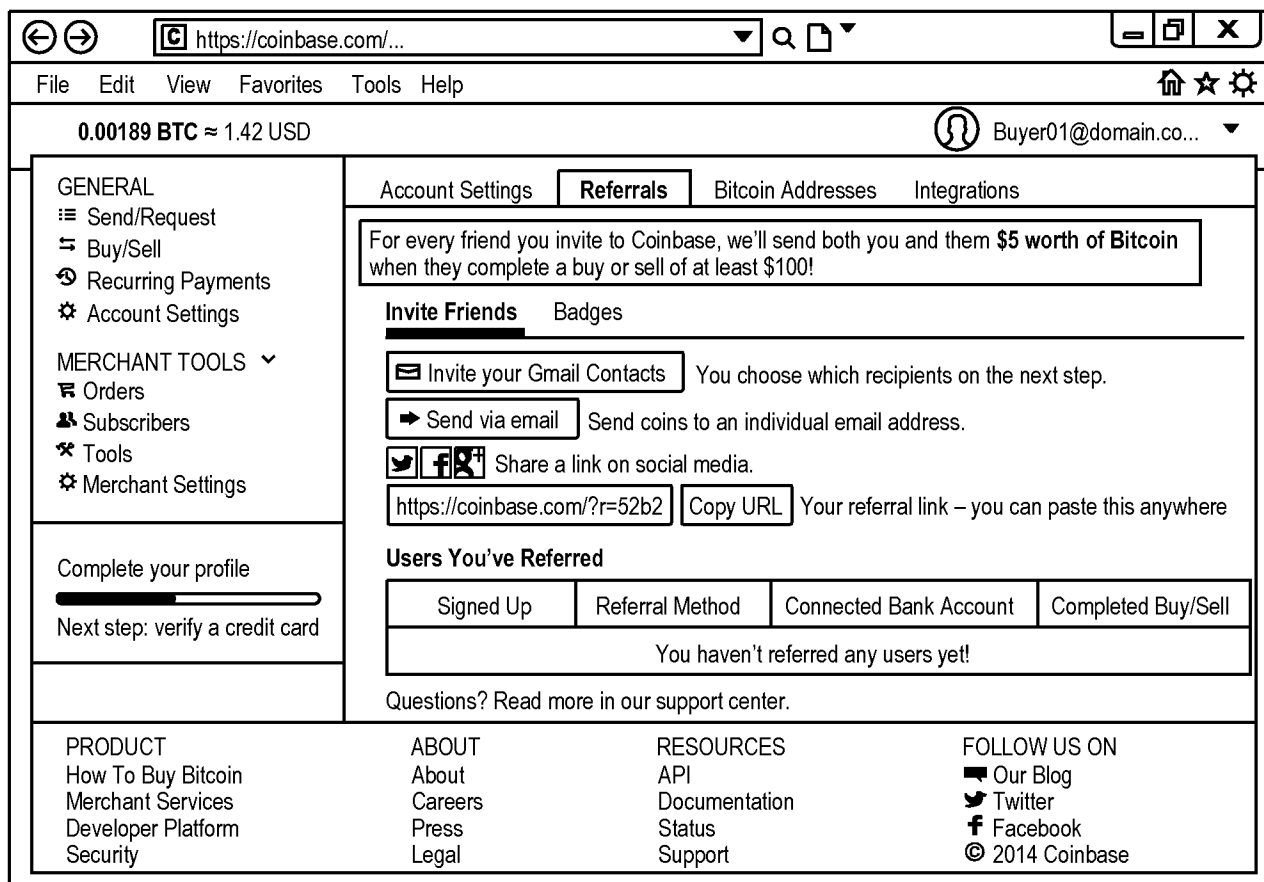


FIG. 31

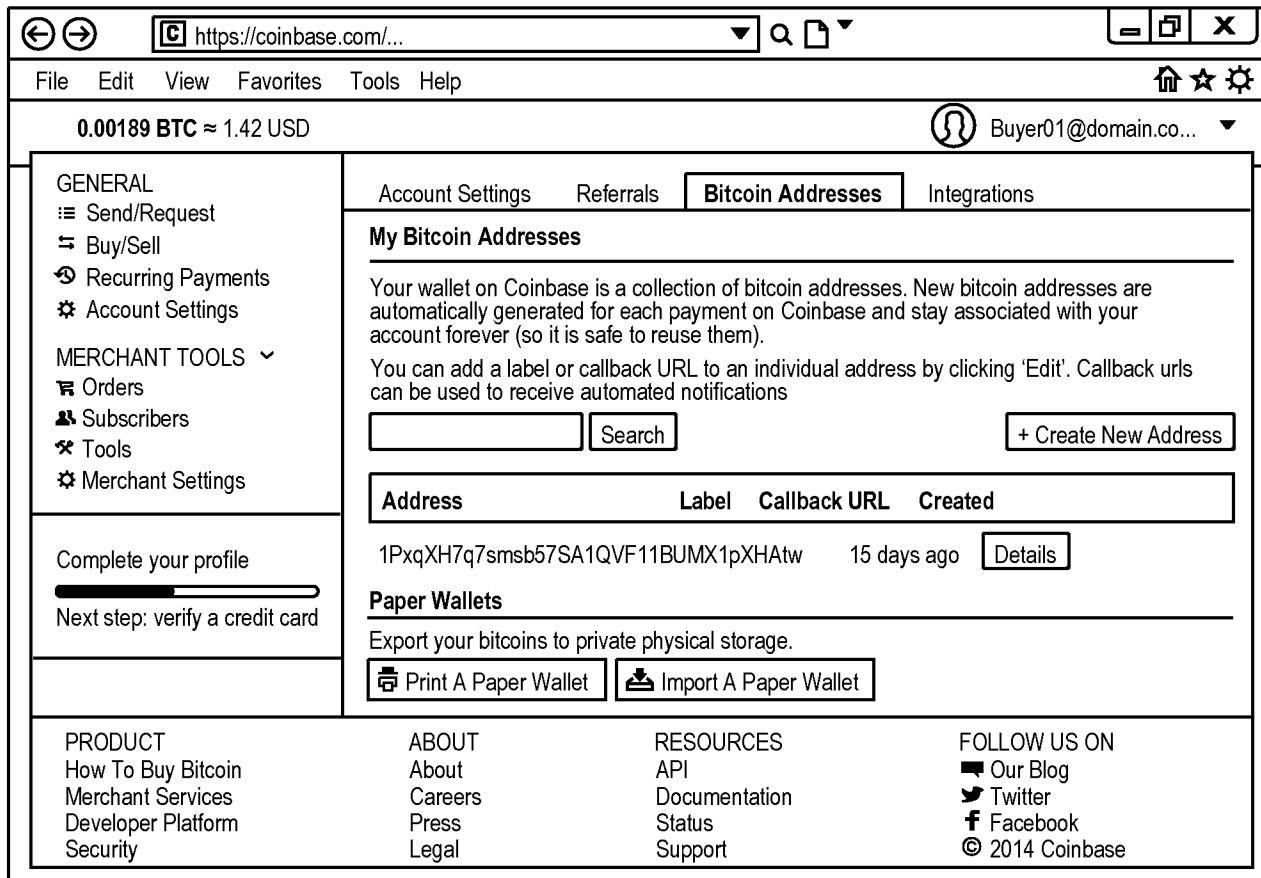


FIG. 32

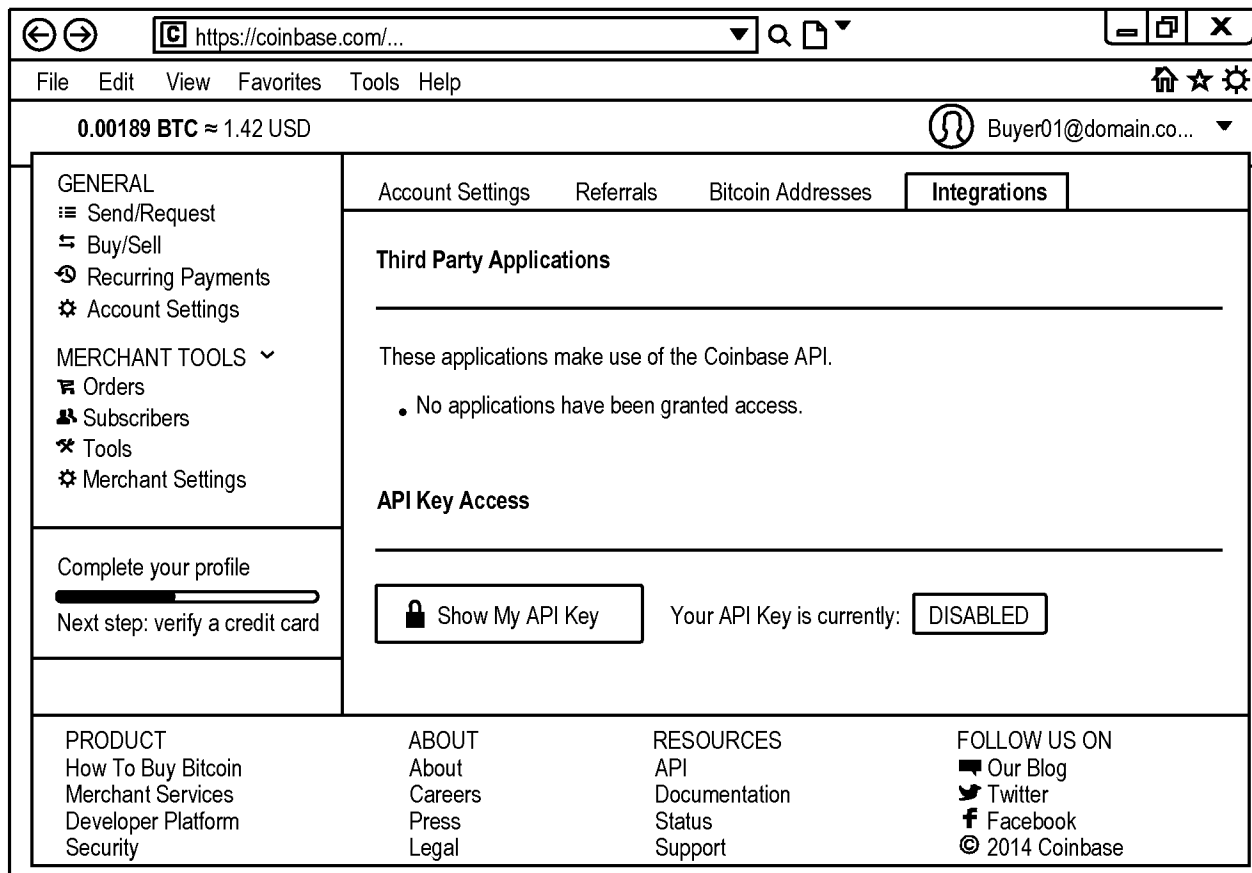


FIG. 33

https://coinbase.com/...

FileEditViewFavoritesToolsHelp

0.00189 BTC ≈ 1.42 USD

Buyer01@domain.co...

GENERAL

- Send/Request
- Buy/Sell
- Recurring Payments
- Account Settings

MERCHANT TOOLS

- Orders
- Subscribers
- Tools
- Merchant Settings

Complete your profile

Next step: verify a credit card

Buy Bitcoin

Sell BitcoinHistoryPayment MethodsLimits and Verifications

Buy Amount

BTC1

×

at \$757.43 USD each

Payment method

Wells Fargo - Bank *****5678

Subtotal

\$757.43

Coinbase fee

\$7.57

Bank fee

\$0.15

Total

\$765.15

Buy Bitcoin

You have 10.0 BTC remaining of your daily buy limit. View limits.

Enable Instant Buy to get your coins in seconds instead of days.

You can also set up a recurring buy.

PRODUCT

- How To Buy Bitcoin
- Merchant Services
- Developer Platform
- Security

ABOUT

- About
- Careers
- Press
- Legal

RESOURCES

- API
- Documentation
- Status
- Support

FOLLOW US ON

- Our Blog
- Twitter
- Facebook
- © 2014 Coinbase

FIG. 34

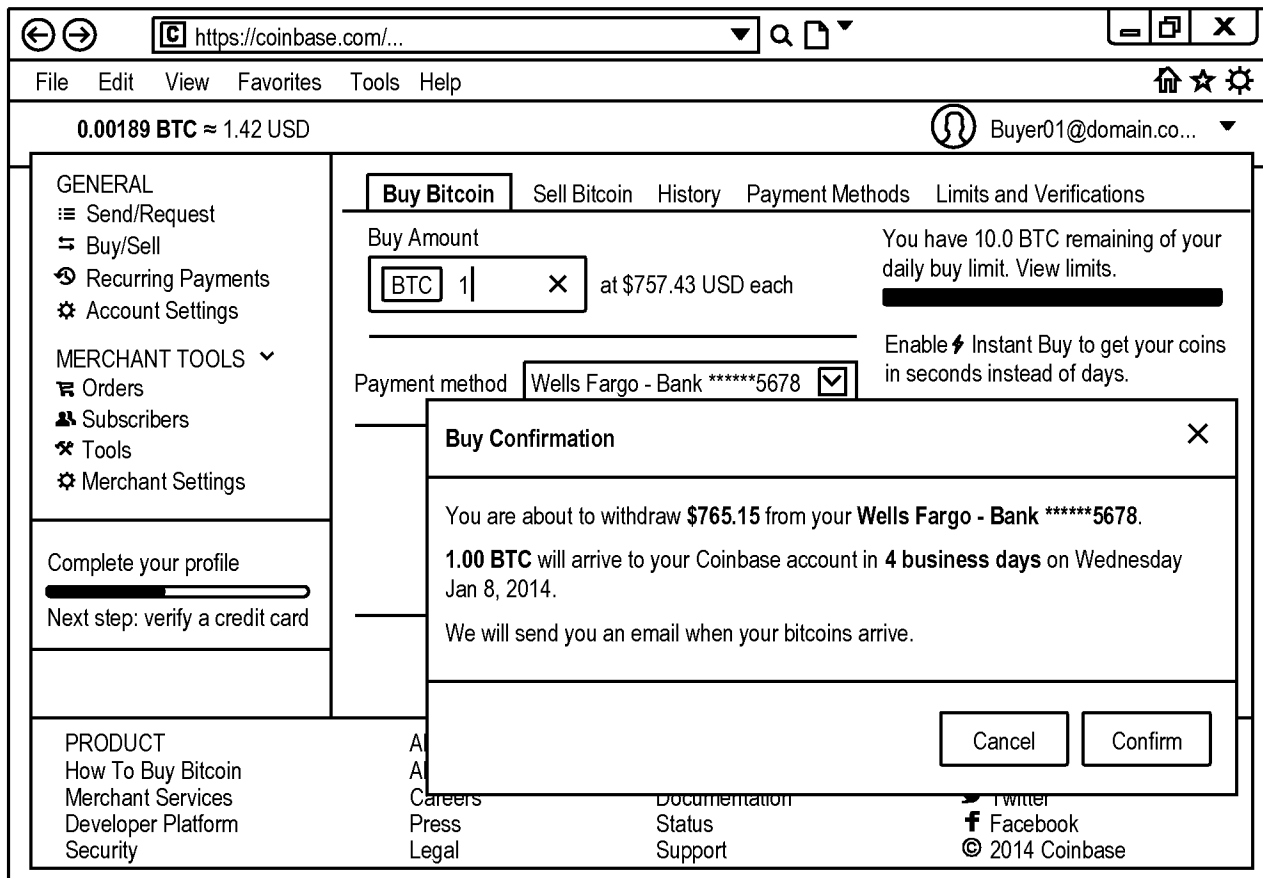


FIG. 35

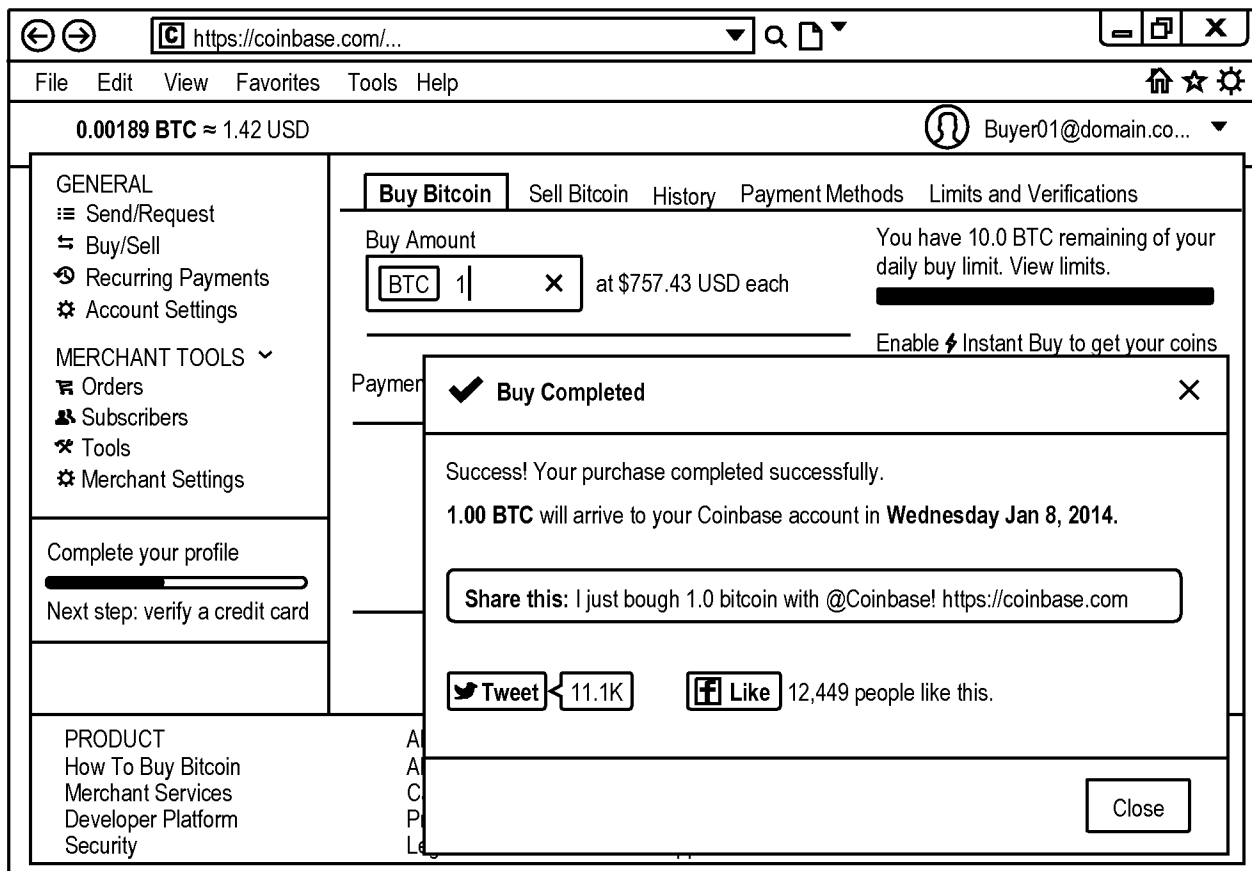


FIG. 36

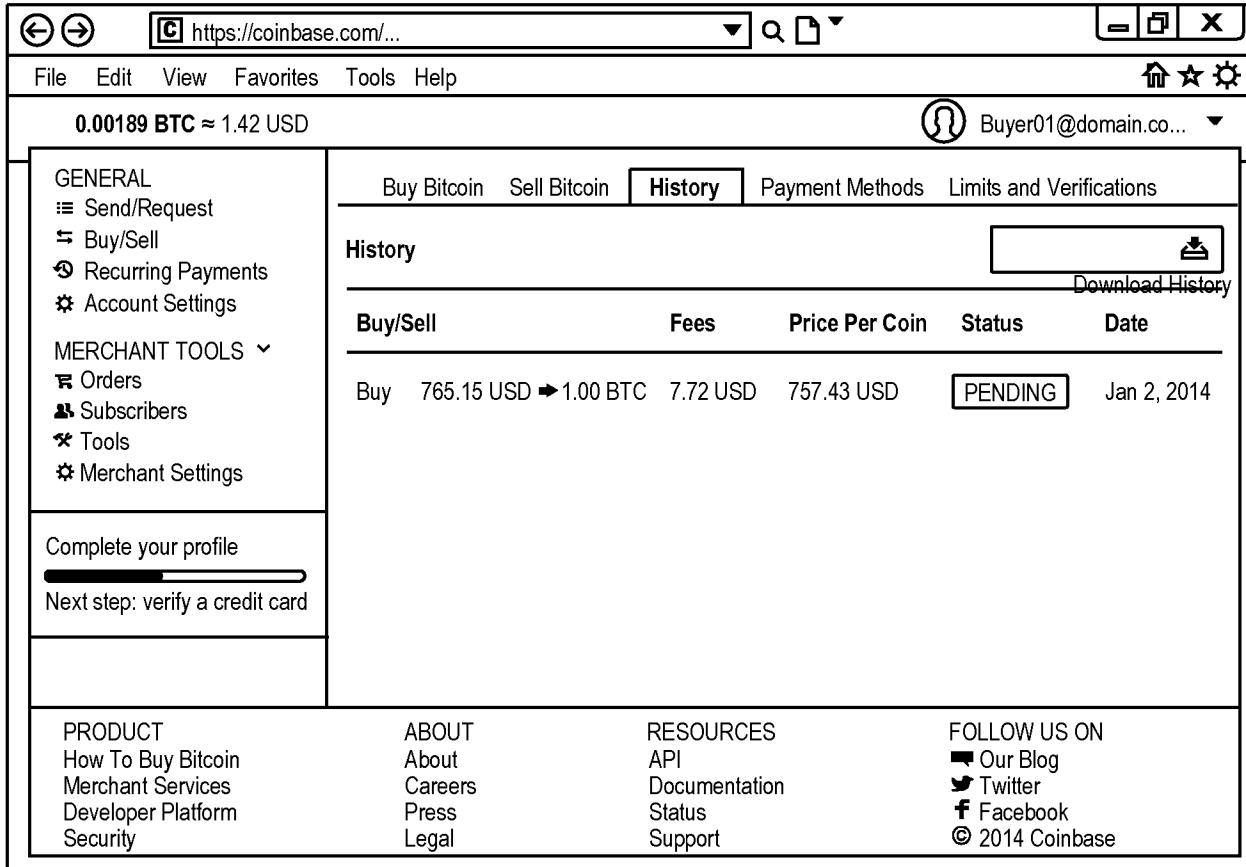


FIG. 37



Hi Buyer01@domain.com

On Jan 2, 2014 you purchased 1.00 BTC via bank transfer.

Those bitcoins are now available in your Coinbase account!

Thank you for the purchase.

Kind regards,
The Coinbase Team

FIG. 38



Hi Buyer01@domain.com

Coinbase just sent you **0.00660667 BTC** (worth \$4.99 USD) using Coinbase.

Attached message:

Congrats! You just earned a referral bonus for completing your first bitcoin purchase/sale. Your friend RepresentativeA also got \$5.00 of bitcoin for telling you about Coinbase.

You and your friends will each receive \$5.00 of bitcoin when you refer them to Coinbase and they buy or sell their first bitcoin. Find out more on the <https://coinbase.com/account/referrals> page.

[Click here to sign in and view this transaction](#)

Kind regards,
The Coinbase Team

FIG. 39

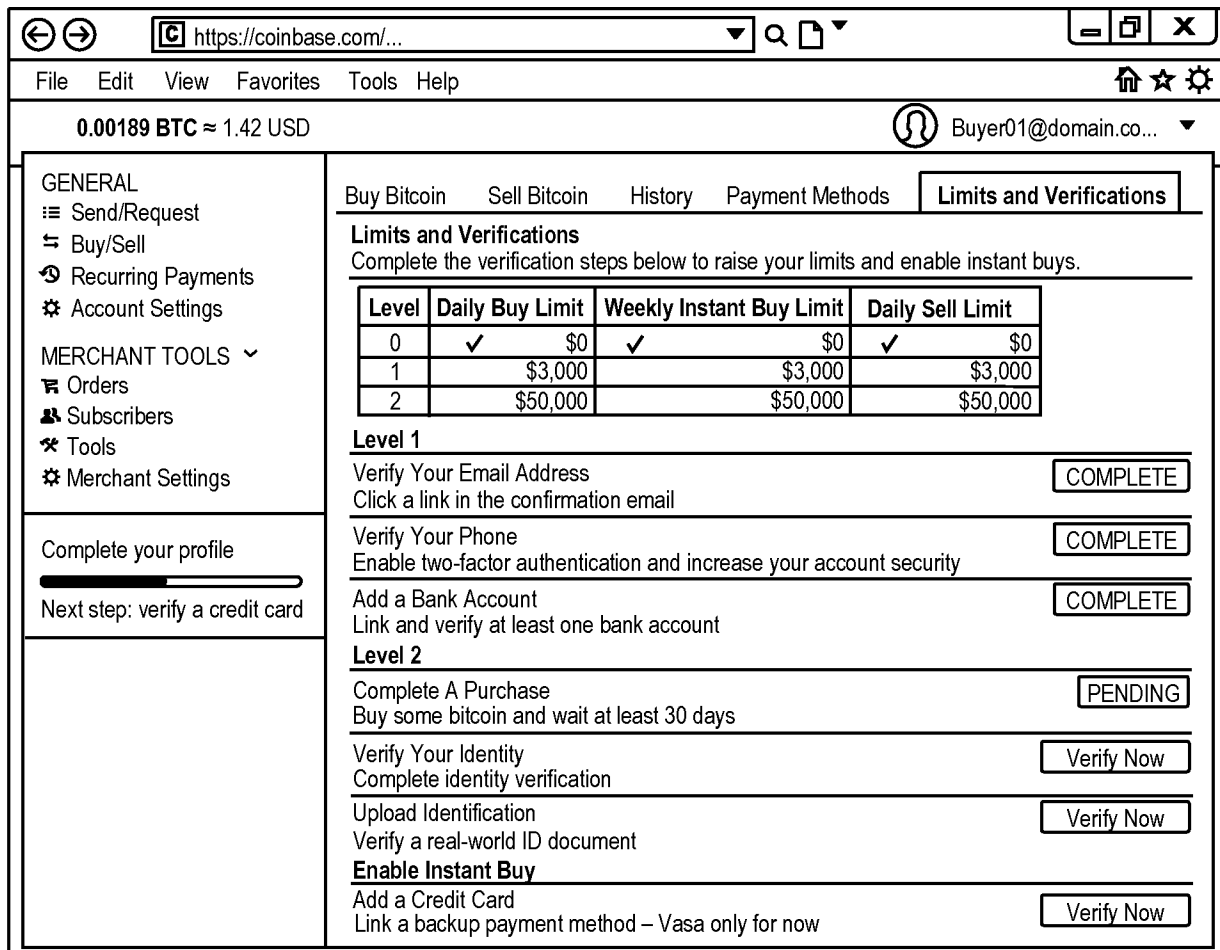


FIG. 40

First Host Computer System 14				
Wallet A			Wallet B	
Email Address A; Login Details			Email address B; Login Details	
Transfer 1	Bitcoin address 1			
		From: First Host		
		Amount in bitcoin		
		Host Fee: x%		
Transfer 2	Bitcoin address 2			
		From: Network address		
		Amount in bitcoin		
		Host Fee: 0 bitcoin		
Transfer 3	Bitcoin address 2		Bitcoin address 3	
		To: Email address B		From: Wallet A
		Amount in bitcoin		Amount in bitcoin
		Miner's Fee = 0 bitcoin		
		Host Fee: 0 bitcoin		
Transfer 4			Bitcoin address 4	
				From: First Host
				Amount in bitcoin
				Host Fee: x%
Transfer 5	Bitcoin address 5		Bitcoin address 4	
		From: Wallet B		To: Email address A
		Amount in bitcoin		Amount in bitcoin
				Miner's Fee = 0 bitcoin
				Host Fee: 0 bitcoin
Transfer 6	Bitcoin address 5		Bitcoin address 4	
		From: Wallet B		To: Bitcoin address 5
		Amount in bitcoin		Amount in bitcoin
				Miner's Fee = 0 bitcoin
				Host Fee: 0 bitcoin

FIG. 41

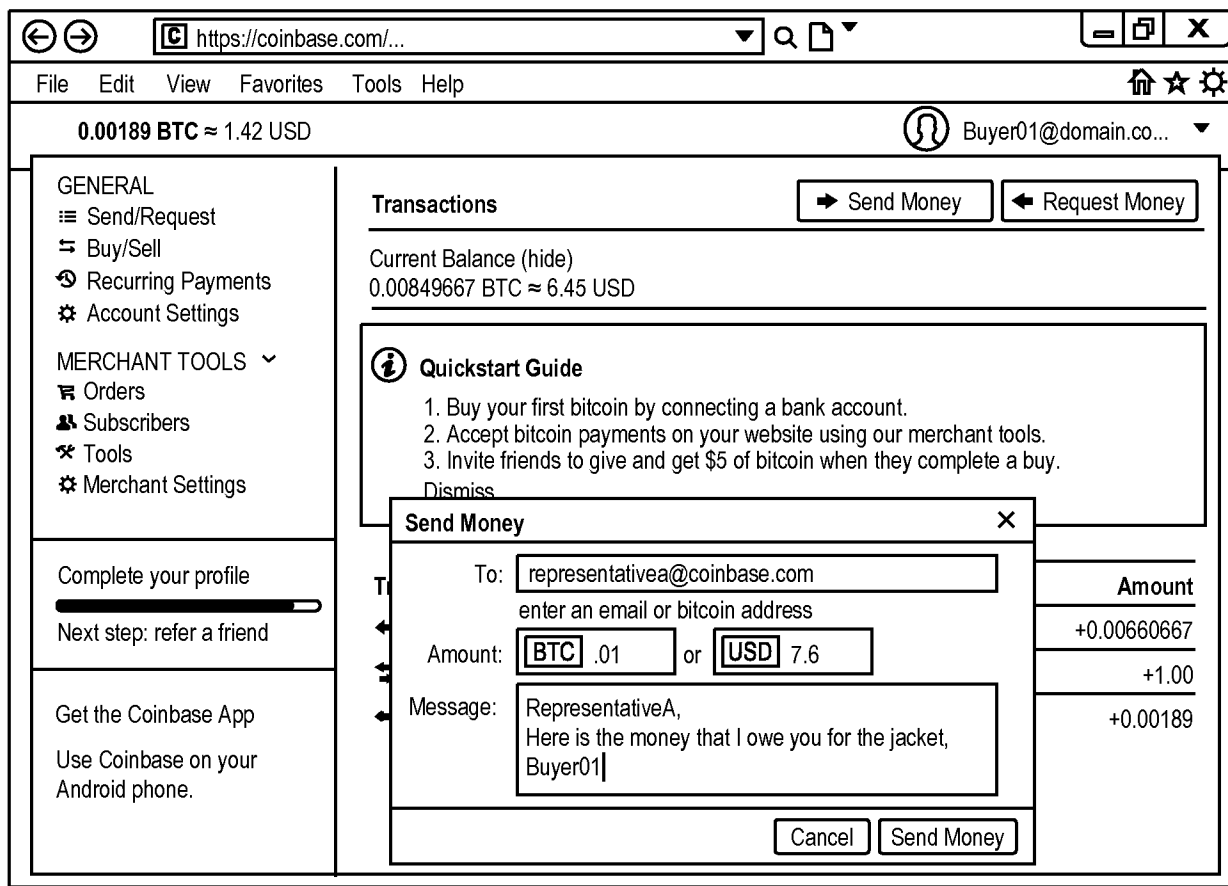


FIG. 42

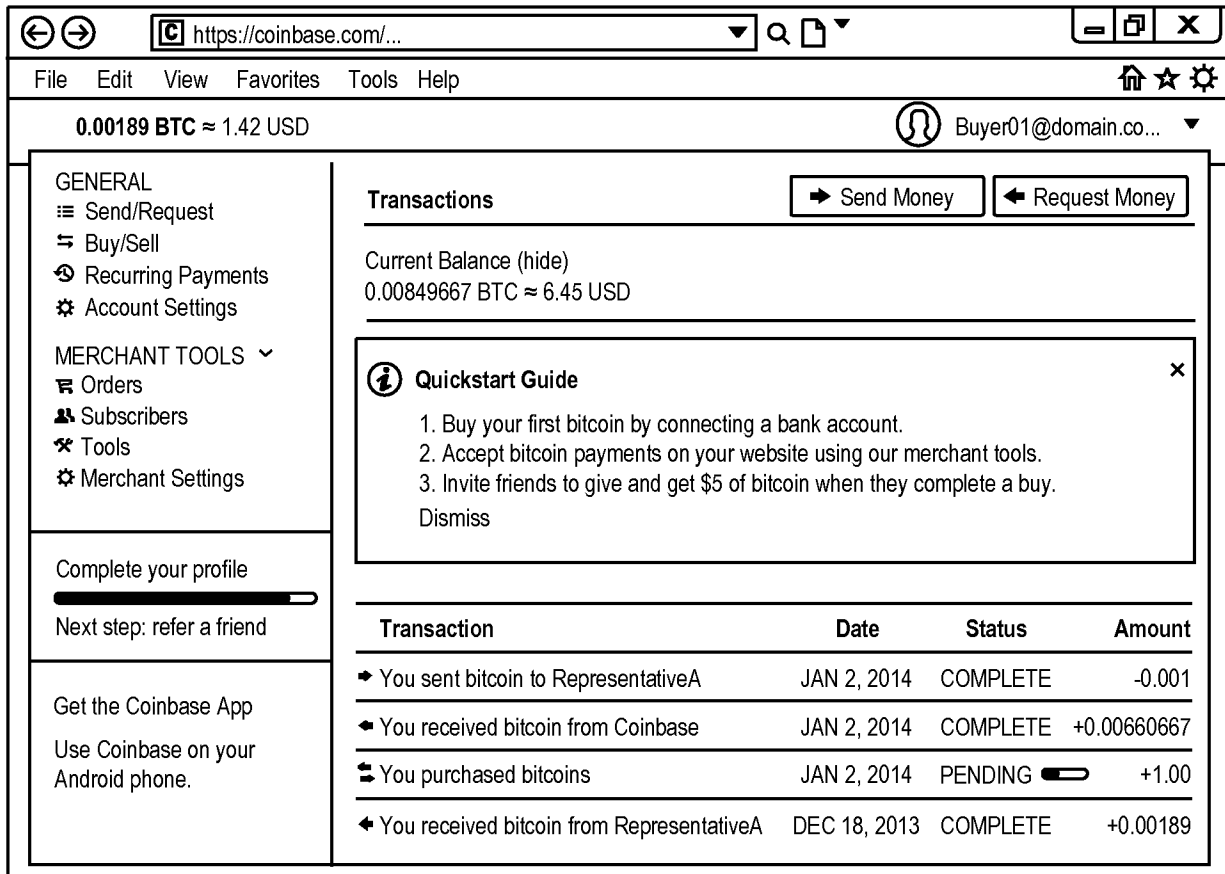


FIG. 43

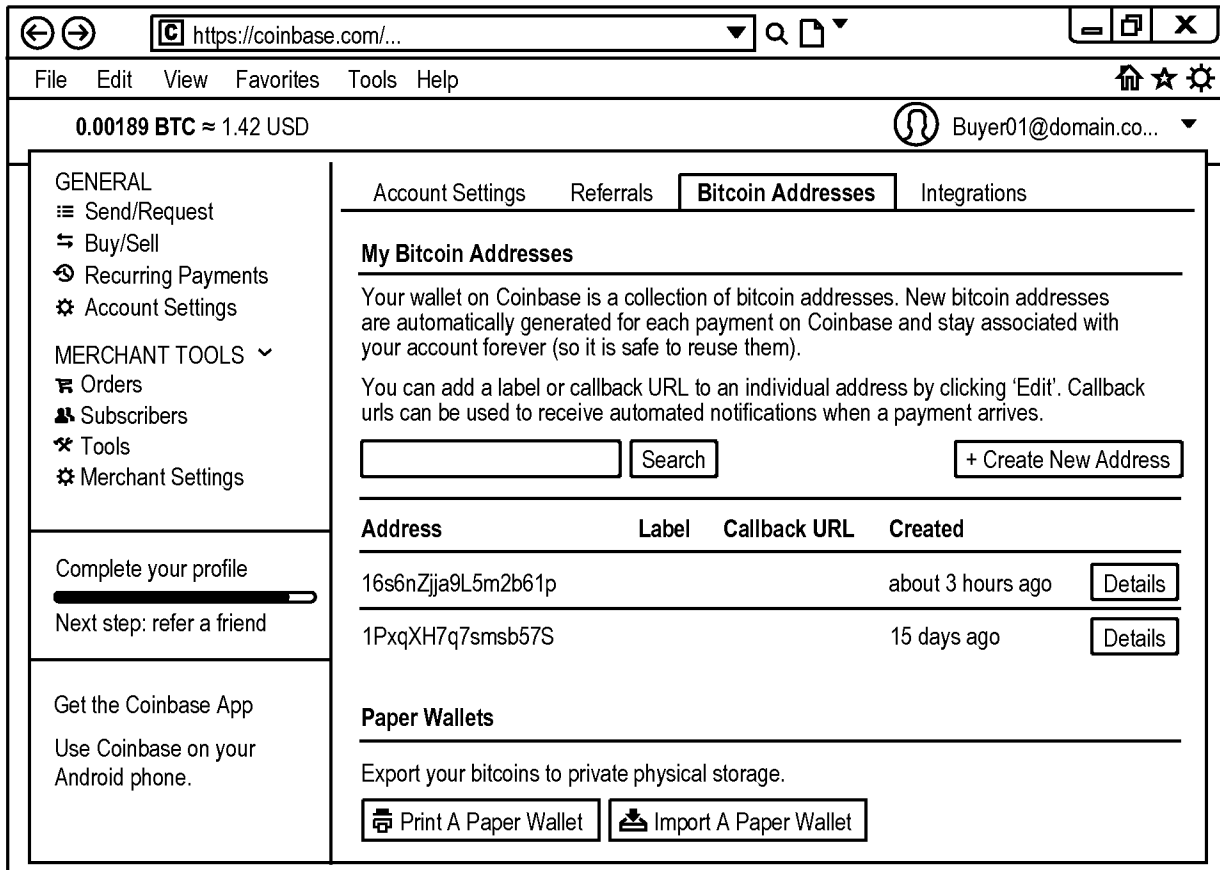


FIG. 44

	First Host Computer System 14			Second Host Computer System 16		
	Wallet A		Wallet B		Wallet C	
	Email Address A; Login Details		Email Address B; Login Details			
Transfer 1	Bitcoin address 1					
		Amount in bitcoin				
	Bitcoin address 2					
Transfer 2		From: Network address				
		Amount in bitcoin				
		Host Fee: 0 bitcoin				
Transfer 3	Bitcoin address 2		Bitcoin address 3			
		To: Email address B		From: Wallet A		
		Amount in bitcoin		Amount in bitcoin		
		Miner's Fee = 0 bitcoin				
		Host Fee: 0 bitcoin				
Transfer 4			Bitcoin address 4			
				From: First Host		
				Amount in bitcoin		
				Host Fee: x%		
Transfer 5	Bitcoin address 5		Bitcoin address 4			
		From: Wallet B		To: Email address A		
		Amount in bitcoin		Amount in bitcoin		
				Miner's Fee = 0 bitcoin		
				Host Fee: 0 bitcoin		
Transfer 6	Bitcoin address 5		Bitcoin address 4			
		From: Wallet B		To: Email address A		
		Amount in bitcoin		Amount in bitcoin		
				Miner's Fee = 0 bitcoin		
				Host Fee: 0 bitcoin		
Transfer 7			Bitcoin address 4		Bitcoin address 6	
				To: Bitcoin Address 6		From: Wallet B (First Host)
				Amount in bitcoin		Amount in bitcoin
				Miner's Fee = 001 Bitcoin		
				Host Fee: 0 bitcoin		

FIG. 45

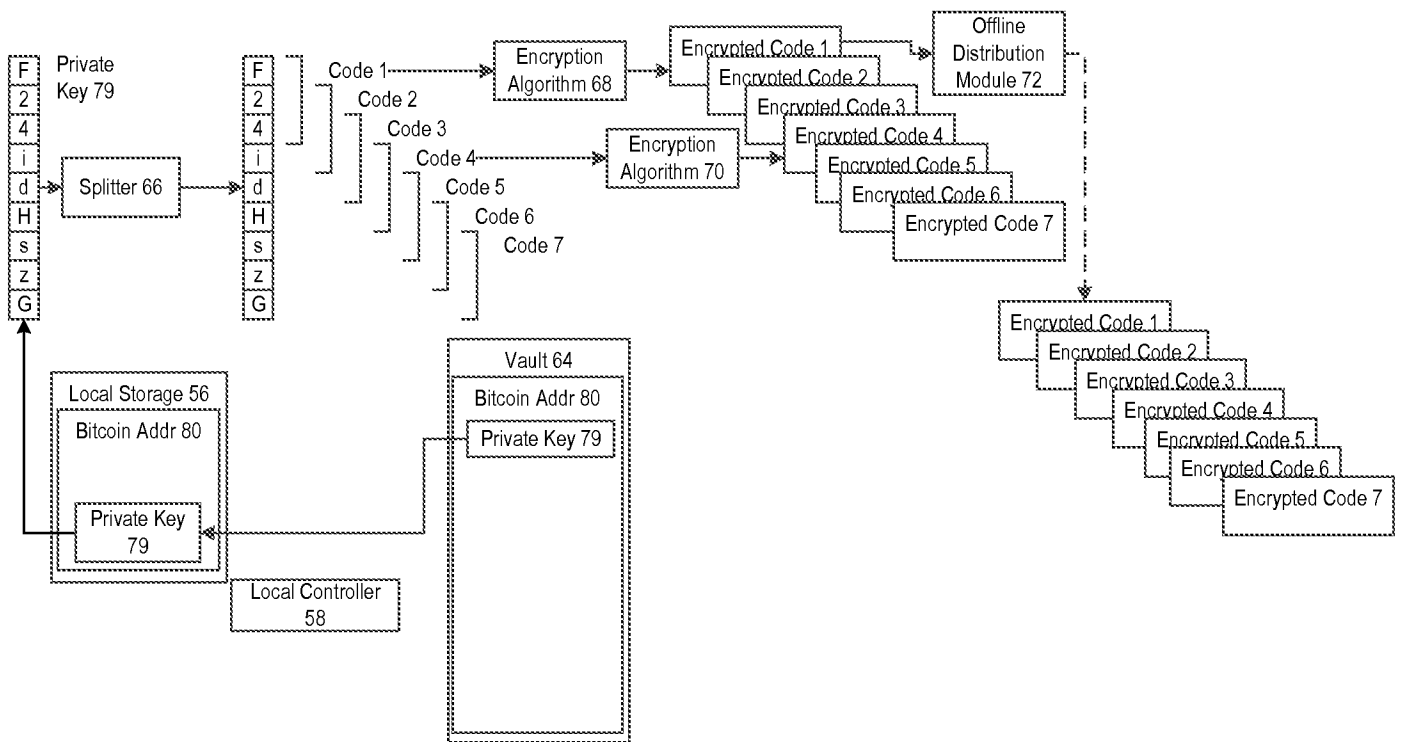


FIG. 46

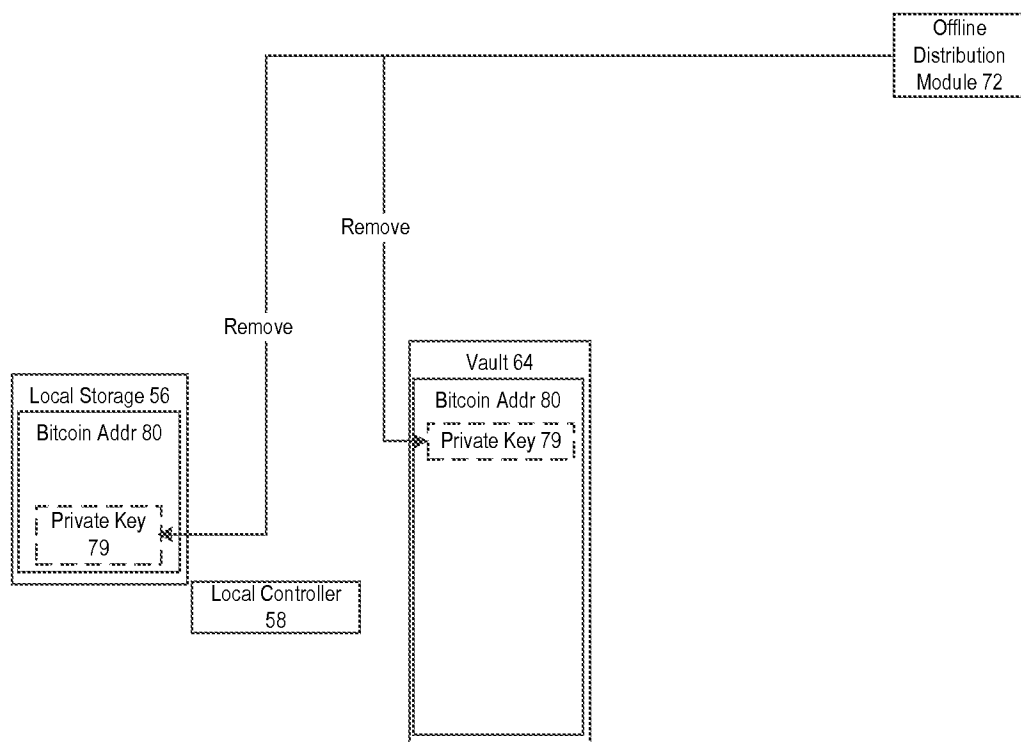


FIG. 47

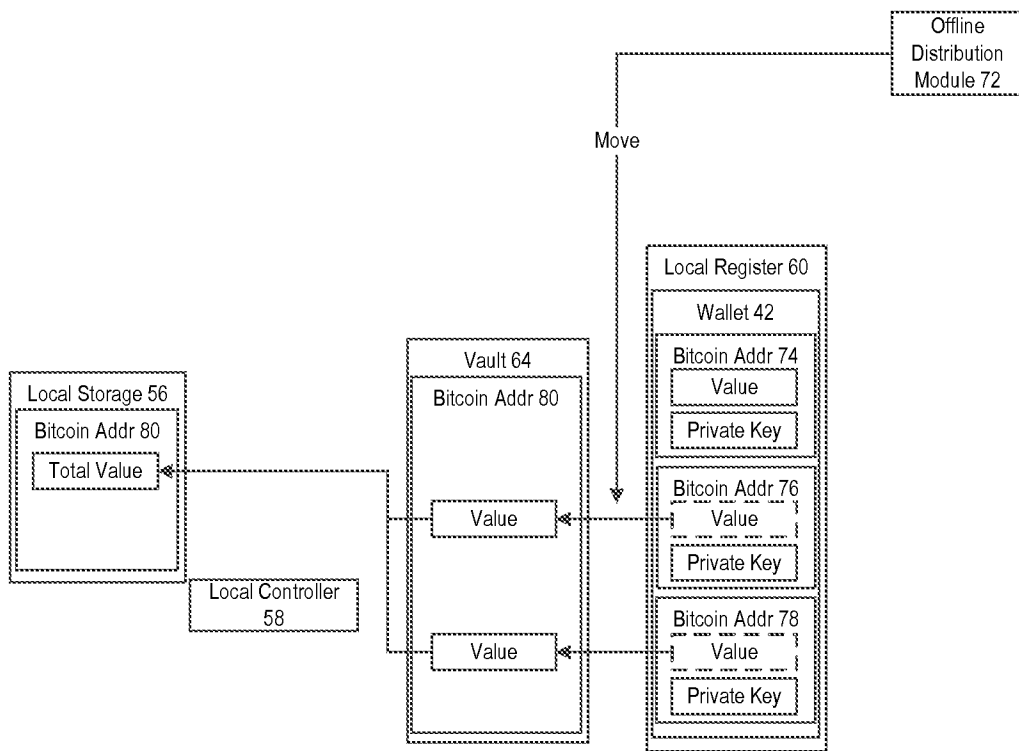


FIG. 48

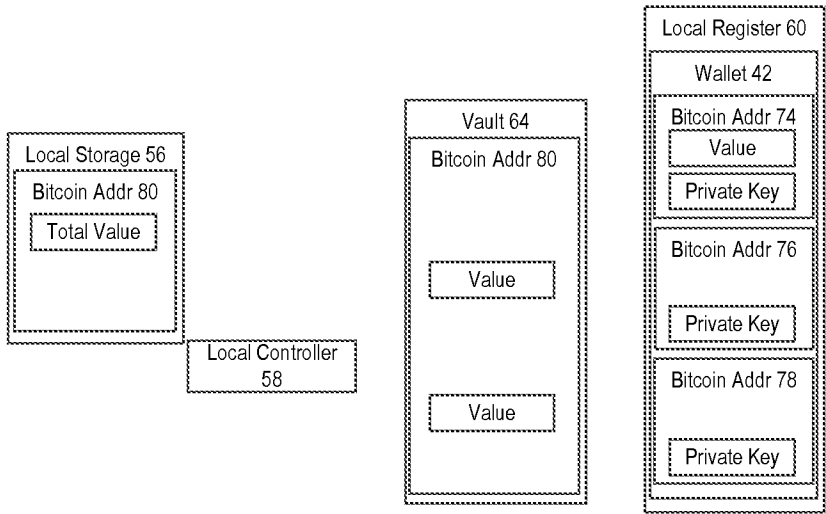


FIG. 49

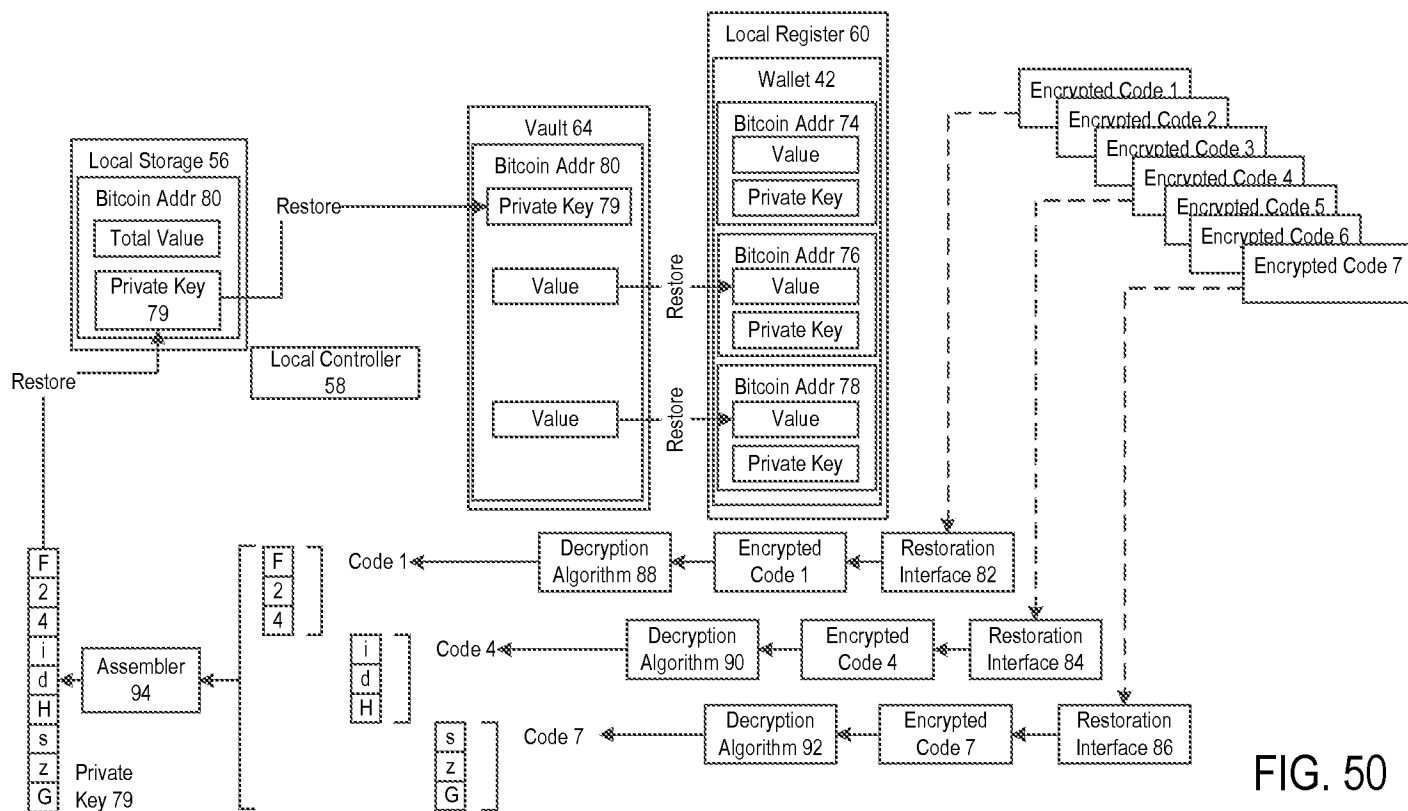


FIG. 50

FIG. 51a

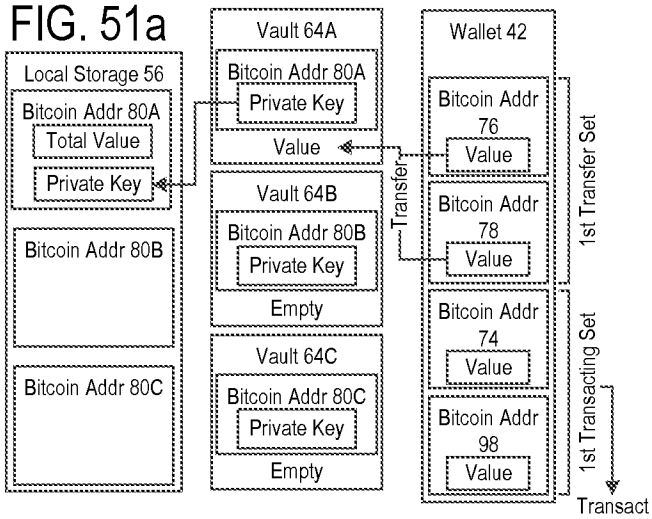


FIG. 51b

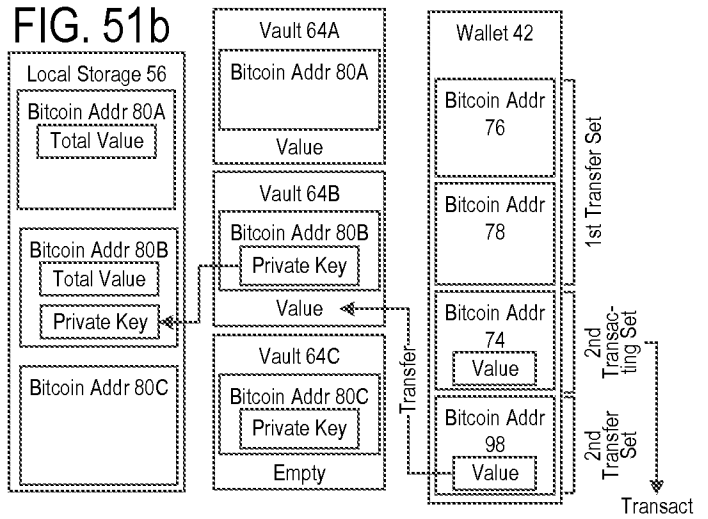


FIG. 51c

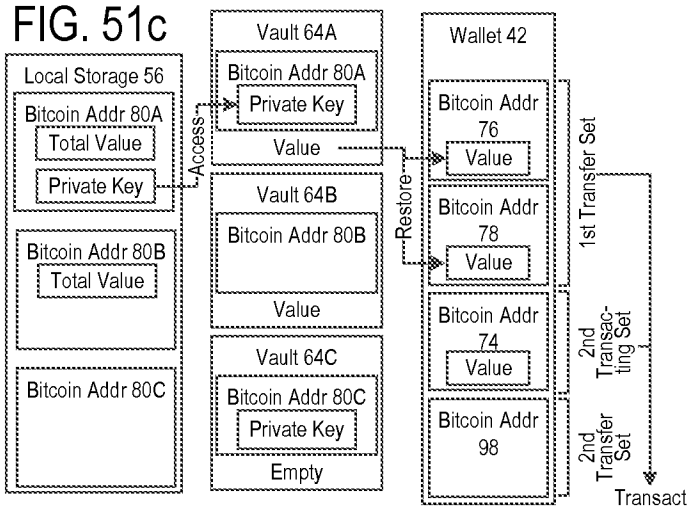
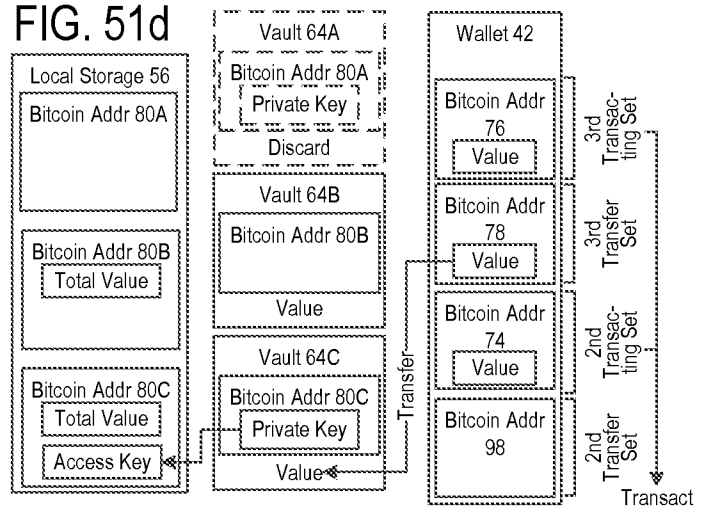


FIG. 51d



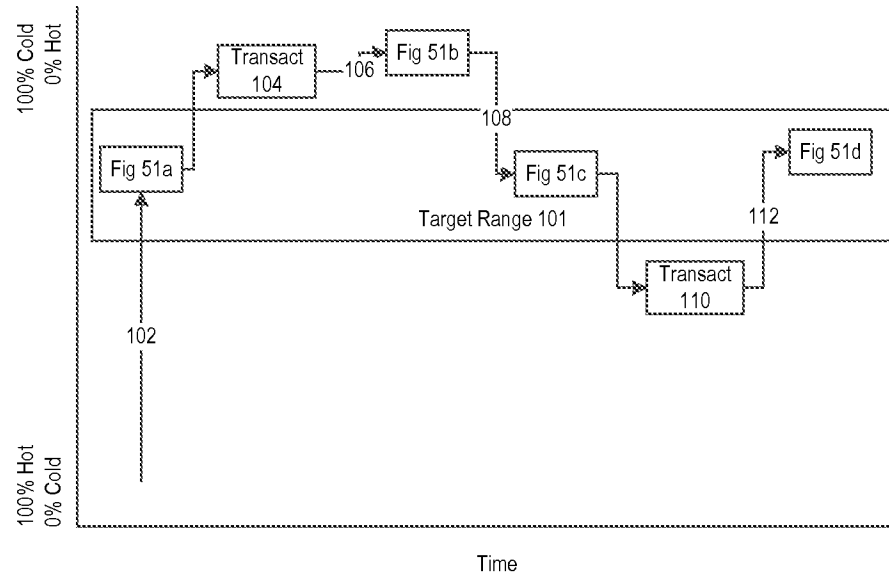


FIG. 52

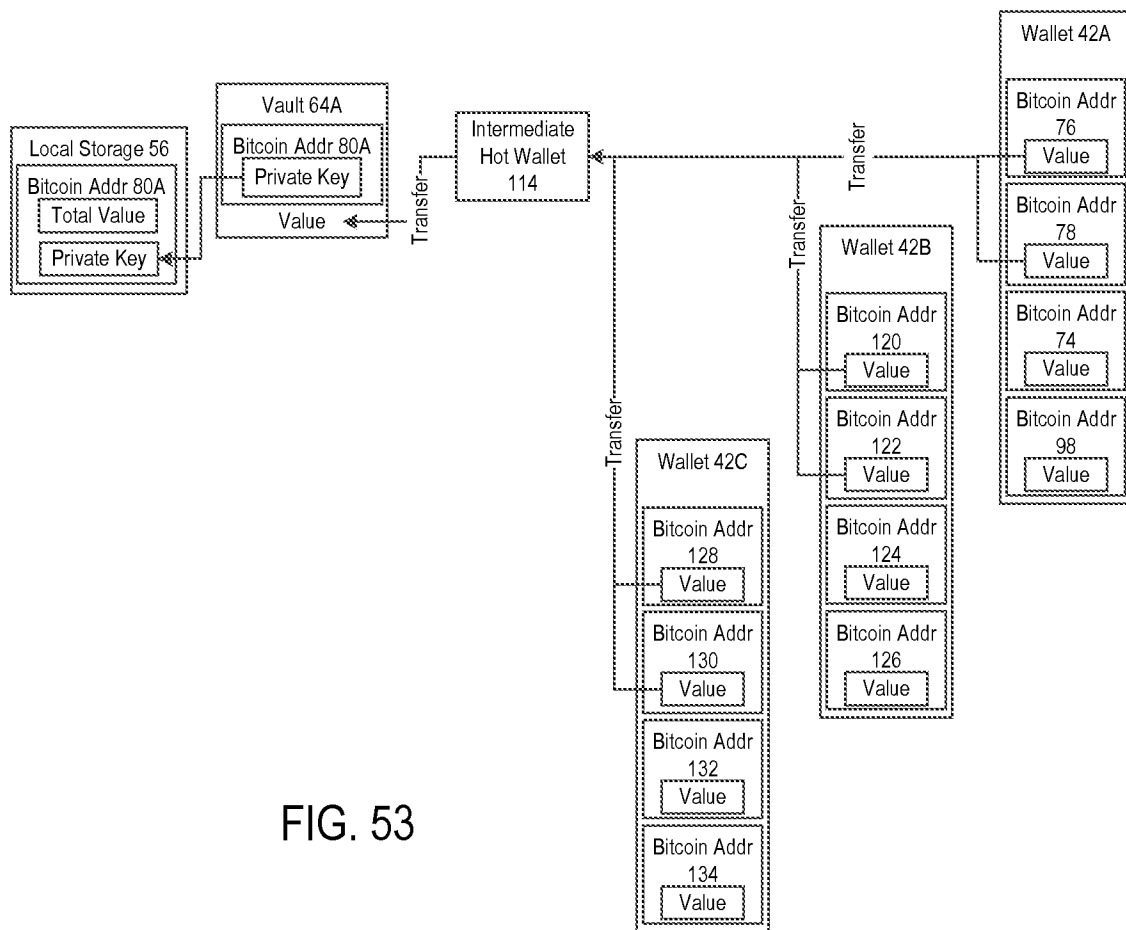


FIG. 53

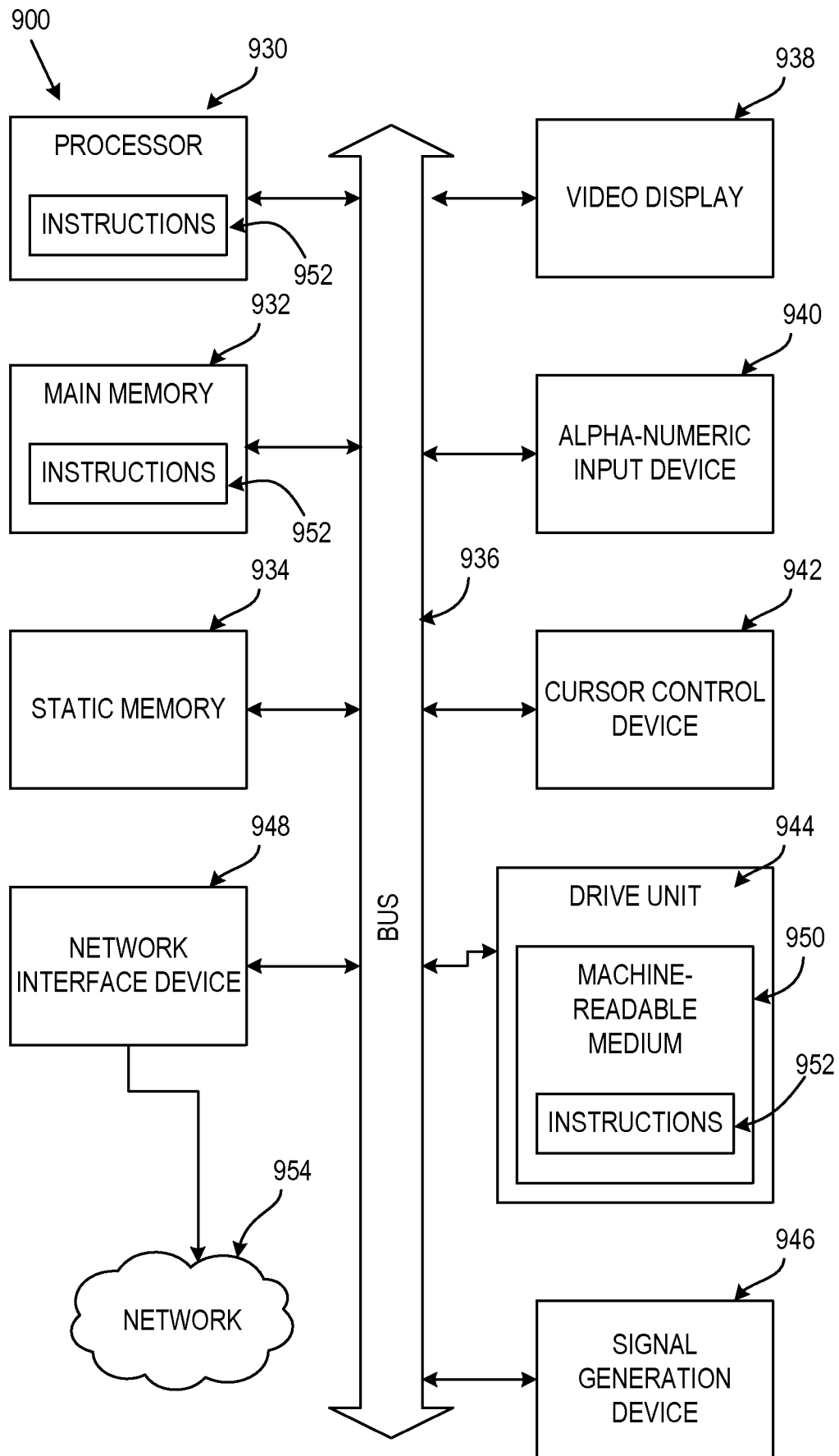


FIG. 54

Electronic Patent Application Fee Transmittal

Application Number:

Filing Date:

Title of Invention:

A METHOD AND SYSTEM FOR TRANSACTING BITCOIN

First Named Inventor/Applicant Name:

Julian Langschaedel

Filer:

Stephen De Klerk.

Attorney Docket Number:

COIN-P002Z

Filed as Small Entity

Provisional Filing Fees

Description

Fee Code

Quantity

Amount

**Sub-Total in
USD(\$)**

Basic Filing:

Provisional Application Filing Fee

2005

1

130

130

Pages:

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				130

Electronic Acknowledgement Receipt

EFS ID:	18973155
Application Number:	61990017
International Application Number:	
Confirmation Number:	5274
Title of Invention:	A METHOD AND SYSTEM FOR TRANSACTING BITCOIN
First Named Inventor/Applicant Name:	Julian Langschaedel
Customer Number:	17169
Filer:	Stephen De Klerk.
Filer Authorized By:	
Attorney Docket Number:	COIN-P002Z
Receipt Date:	07-MAY-2014
Filing Date:	
Time Stamp:	19:38:05
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	5333
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Provisional Cover Sheet (SB16)	COIN- P002Z_Provisional_Cover_Sheet_050714.pdf	92431 29d776ef080fb288c4b7b88dec35499c96e63691	no	3
Warnings:					
This is not a USPTO supplied Provisional Cover Sheet SB16 form.					
Information:					
2	Application Data Sheet	COIN-P002Z_ADS_050714.pdf	133135 87f990fcb241cc6e536ac11707022e21d4a2d7af	no	7
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3		COIN- P002Z_Provisional_Application_050714.pdf	216726 4309bfee659915bf12136b822b096bf55d51b712	yes	59
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	32	
	Claims		33	58	
	Abstract		59	59	
Warnings:					
Information:					
4	Drawings-only black and white line drawings	COIN-P002Z_Figures_As_Filed.pdf	454868 b69dde26bdc76de3621dcf2d442d96b8bc b5c1a9	no	53
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	29583 431341d16ee0af385a84a2564be01ae8cc40b1fa	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			926743		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.