United States Patent	12388619
Kind Code	B2
Date of Patent	August 12, 2025
Inventor(s)	Walters; Austin Grant et al.

System and method for authorizing transactions in an authorized member network

Abstract

In the disclosed transaction processing system, members of an authorized network of consumers and merchants manage account information using blockchain ledgers. Because both consumers and merchants maintain copies of the blockchain, for any consumer/merchant transaction, both entities can quickly validate the transaction because both are aware, via their blockchain entries, of the current status of the account sourcing the transaction, allowing fast and accurate transaction validation without the need to incur the processing charges inherent in traditional fiat currency credit transactions.

Inventors: **Walters; Austin Grant (Savoy, IL), Farivar; Reza (Champaign, IL), Goodsitt; Jeremy Edward (Champaign, IL)**

Applicant: **Capital One Services, LLC** (McLean, VA)

Family ID: **1000008750580**

Assignee: **Capital One Services, LLC (McLean, VA)**

Appl. No.: **17/580945**

Filed: **January 21, 2022**

Prior Publication Data

Document Identifier	Publication Date
US 20220255725 A1	Aug. 11, 2022

Related U.S. Application Data

continuation parent-doc US 16822928 20200318 US 11245513 child-doc US 17580945
continuation parent-doc US 16230106 20181221 US 10637644 20200428 child-doc US 16822928

Publication Classification

Int. Cl.: **H04L9/08** (20060101); **G06F16/23** (20190101); **G06Q20/06** (20120101); **G06Q20/20** (20120101); **H04L9/00** (20220101); **H04L9/06** (20060101)

U.S. Cl.:

CPC **H04L9/0618** (20130101); **G06F16/2365** (20190101); **G06Q20/065** (20130101); **G06Q20/20** (20130101); **H04L9/006** (20130101); **H04L9/0833** (20130101); H04L9/50 (20220501)

Field of Classification Search

CPC: H04L (9/0618); H04L (9/006); H04L (9/0833); H04L (9/50); H04L (9/3239); G06F (16/2365); G06Q (20/065); G06Q (20/20); G06Q (20/02); G06Q (2220/00); G06Q (20/401)

References Cited

U.S. PATENT DOCUMENTS

Patent No.	**Issued Date**	**Patentee Name**	**U.S. Cl.**	**CPC**
5535407	12/1995	Yanagawa	235/380	G06Q 20/10
5953709	12/1998	Gilbert	194/347	G06Q 20/20
RE40444	12/2007	Linehan	713/172	G06Q 20/02
8060598	12/2010	Cook	709/224	H04L 45/16
8266066	12/2011	Wezter	703/20	G06Q 10/06
8886570	12/2013	Amancherla	235/382	G06Q 20/4016
9741036	12/2016	Grassadonia	N/A	G06Q 20/405
10031993	12/2017	Poornachandran	N/A	H03K 19/17704
10055715	12/2017	Grassadonia	N/A	G06Q 20/36
10084762	12/2017	Versteeg	N/A	H04L 63/08
10102265	12/2017	Madisetti	N/A	G06F 16/27
10250694	12/2018	Mankovskii	N/A	H04L 67/535
10554649	12/2019	Fields	N/A	H04L 9/3263
10762506	12/2019	Cash	N/A	G06Q 20/206
11126613	12/2020	Ow	N/A	G06F 16/137
2001/0025262	12/2000	Ahmed	705/33	G06Q 40/128
2002/0179401	12/2001	Knox	194/217	G06Q 20/28
2004/0024795	12/2003	Hind	N/A	G06F 16/275
2004/0083149	12/2003	Jones	705/35	G06Q 40/00
2004/0122699	12/2003	Brito	705/301	G06Q 10/103
2005/0154751	12/2004	Levi	707/999.102	G06Q 10/10
2006/0094499	12/2005	Amemiya	463/29	A63F 13/71
2006/0131392	12/2005	Cooper	235/380	G06Q 20/24
2006/0149671	12/2005	Nix	705/40	G06Q 20/24
2007/0045407	12/2006	Paul	235/380	G06Q 20/14
2007/0125838	12/2006	Law	705/65	G07F 7/1008

2007/0125840	12/2006	Law	705/65	G06Q 20/363
2008/0228647	12/2007	Kachel	705/42	G06Q 30/04
2008/0249848	12/2007	Kay	705/14.39	G06Q 30/0239
2008/0249926	12/2007	Sgaraglio	705/30	G06Q 40/00
2009/0172035	12/2008	Lessing	N/A	G06Q 30/02
2009/0293104	12/2008	Levi	726/4	G06Q 10/10
2009/0299909	12/2008	Levi	705/37	G06Q 10/06
2013/0179186	12/2012	Birtwhistle	705/3	G16H 10/60
2014/0222632	12/2013	Dhakephalkar	705/30	G06Q 40/12
2014/0310172	12/2013	Grossman	705/44	G06Q 20/10
2015/0120539	12/2014	Amancherla	705/41	G06Q 20/40
2015/0186485	12/2014	Guo	707/624	H04L 67/1095
2015/0278796	12/2014	Jiang	705/44	G06Q 20/3825
2015/0332256	12/2014	Minor	N/A	N/A
2015/0348009	12/2014	Brown	N/A	N/A
2015/0363769	12/2014	Ronca	N/A	N/A
2015/0371224	12/2014	Lingappa	705/71	G06Q 20/065
2016/0042485	12/2015	Kopel	705/13	G07B 15/04
2016/0260169	12/2015	Arnold	N/A	G06Q 20/381
2016/0267605	12/2015	Lingham	N/A	G06Q 40/12
2016/0335628	12/2015	Weigold	N/A	G06Q 20/065
2016/0342976	12/2015	Davis	N/A	G06Q 20/10
2016/0342978	12/2015	Davis	N/A	G06Q 20/0655
2016/0342989	12/2015	Davis	N/A	H04L 9/50
2016/0342994	12/2015	Davis	N/A	G06Q 40/02
2017/0004506	12/2016	Steinman	N/A	G06Q 20/3827
2017/0046806	12/2016	Haldenby	N/A	G06Q 40/08
2017/0053249	12/2016	Tunnell	N/A	G09C 5/00
2017/0091753	12/2016	May	N/A	N/A
2017/0161734	12/2016	Bankston	N/A	G06Q 20/3829
2017/0213209	12/2016	Dillenberger	N/A	G06F 16/2322
2017/0230189	12/2016	Toll	N/A	G06F 21/57
2017/0235970	12/2016	Conner	707/690	G06F 21/44
2017/0236121	12/2016	Lyons	705/71	G06Q 20/06
2017/0243212	12/2016	Castinado	N/A	G06Q 20/389
2017/0243214	12/2016	Johnsrud	N/A	G06Q 40/03
2017/0243217	12/2016	Johnsrud	N/A	G06Q 20/4014
2017/0243222	12/2016	Balasubramanian	N/A	G06Q 20/4014
2017/0243286	12/2016	Castinado	N/A	H04L 9/3239
2017/0243287	12/2016	Johnsrud	N/A	G06Q 20/02

2017/0249354	12/2016	Lee	N/A	G06F 16/2358
2017/0249608	12/2016	Rooke	N/A	G06Q 40/02
2017/0250972	12/2016	Ronda	N/A	H04L 9/0891
2017/0270482	12/2016	Mohun	N/A	G06Q 10/103
2017/0344983	12/2016	Muftic	N/A	G06Q 20/065
2017/0351464	12/2016	Mashiko	N/A	G06F 3/1204
2017/0357966	12/2016	Chandrasekhar	N/A	G06Q 20/06
2017/0357970	12/2016	Muftic	N/A	G06Q 20/24
2017/0372417	12/2016	Gaddam	N/A	G06Q 20/06
2018/0005203	12/2017	Grassadonia	N/A	G06Q 20/40
2018/0005229	12/2017	Grassadonia	N/A	G06Q 40/04
2018/0018380	12/2017	Saxena	N/A	G06F 16/27
2018/0018723	12/2017	Nagla	N/A	H04L 63/102
2018/0025442	12/2017	Isaacson	705/26.62	H04L 51/48
2018/0032383	12/2017	Surcouf	N/A	H04L 9/3239
2018/0039667	12/2017	Pierce	N/A	H04L 9/3247
2018/0046992	12/2017	Hanrahan	N/A	G06Q 20/02
2018/0054491	12/2017	Mankovskii	N/A	H04L 67/142
2018/0063099	12/2017	Versteeg	N/A	H04W 12/04
2018/0068130	12/2017	Chan	N/A	G06F 21/606
2018/0075453	12/2017	Durvasula	N/A	G06Q 20/3678
2018/0075527	12/2017	Nagla	N/A	G06F 21/6218
2018/0082359	12/2017	Hilmola	N/A	G06F 16/58
2018/0083786	12/2017	Dierks	N/A	H04L 9/3297
2018/0089641	12/2017	Chan	N/A	G06Q 40/06
2018/0091524	12/2017	Setty	N/A	H04L 9/3247
2018/0101914	12/2017	Samuel	N/A	G06Q 20/401
2018/0121911	12/2017	Hallam	N/A	G06Q 20/10
2018/0150488	12/2017	Runchey	N/A	H04L 67/10
2018/0150865	12/2017	Arora	N/A	G06Q 20/3678
2018/0158051	12/2017	Arora	N/A	G06Q 20/3829
2018/0158139	12/2017	Krajicek	N/A	G06Q 30/04
2018/0189781	12/2017	McCann	N/A	G06Q 20/202
2018/0191714	12/2017	Jentzsch	N/A	G06F 21/445
2018/0197173	12/2017	Durvasula	N/A	G06Q 20/3823
2018/0218176	12/2017	Voorhees	N/A	N/A
2018/0225640	12/2017	Chapman	N/A	G06Q 20/401
2018/0225660	12/2017	Chapman	N/A	G06Q 20/10
2018/0254887	12/2017	Ateniese	N/A	G06F 3/0673
2018/0268401	12/2017	Ortiz	N/A	G06Q 20/326
2018/0276666	12/2017	Haldenby	N/A	H04L 9/3268
2018/0276710	12/2017	Tietzen	N/A	G06Q 30/0269
2018/0285839	12/2017	Yang	N/A	G06Q 20/40

2018/0293553	12/2017	Dembo	N/A	G06Q 20/381
2018/0308117	12/2017	Gupta	N/A	G06Q 30/0226
2018/0308134	12/2017	Manning	N/A	G06Q 30/0277
2018/0315027	12/2017	Kumar	N/A	G06Q 20/3278
2019/0005469	12/2018	Dhupkar	N/A	H04L 9/3236
2019/0005491	12/2018	Grassadonia	N/A	G06Q 20/4014
2019/0012695	12/2018	Bishnoi	N/A	G06Q 20/223
2019/0018888	12/2018	Madisetti	N/A	G06F 16/27
2019/0020468	12/2018	Rosenoer	N/A	H04L 9/3228
2019/0028276	12/2018	Pierce	N/A	G06Q 20/3825
2019/0034888	12/2018	Grassadonia	N/A	G06Q 20/065
2019/0034903	12/2018	Arora	N/A	G06Q 20/02
2019/0057379	12/2018	Chalakudi	N/A	H04L 63/12
2019/0058590	12/2018	Watanabe	N/A	G06Q 20/065
2019/0068562	12/2018	Iyer	N/A	H04L 9/0637
2019/0073666	12/2018	Ortiz	N/A	H04L 9/3236
2019/0080406	12/2018	Molinari	N/A	G06Q 40/02
2019/0081789	12/2018	Madisetti	N/A	H04L 9/0637
2019/0088062	12/2018	Unagami	N/A	G06F 21/31
2019/0088063	12/2018	Unagami	N/A	G06F 21/10
2019/0104102	12/2018	Khan	N/A	G06F 16/27
2019/0114182	12/2018	Chalakudi	N/A	H04L 63/0442
2019/0116142	12/2018	Chalakudi	N/A	H04L 51/046
2019/0156363	12/2018	Postrel	N/A	H04L 67/566
2019/0172021	12/2018	Watson	N/A	G06Q 40/02
2019/0172026	12/2018	Vessenes	N/A	G06Q 20/065
2019/0220856	12/2018	Li	N/A	N/A
2019/0229926	12/2018	Handa	N/A	G06Q 20/40
2019/0238550	12/2018	Zhang	N/A	H04L 63/105
2019/0251187	12/2018	Lin	N/A	G06F 16/1834
2019/0268141	12/2018	Pandurangan	N/A	H04L 67/1023
2019/0286805	12/2018	Law	N/A	G06F 21/34
2019/0305958	12/2018	Qiu	N/A	G06Q 20/389
2019/0305966	12/2018	Qiu	N/A	H04L 9/3239
2019/0306235	12/2018	Veale	N/A	H04L 63/123
2019/0347658	12/2018	Haimes	N/A	G06Q 20/401
2019/0361874	12/2018	Fukuchi	N/A	H04L 9/12
2020/0027067	12/2019	Hertzog	N/A	N/A
2020/0050774	12/2019	Unagami	N/A	H04L 9/3247
2020/0051071	12/2019	Wu	N/A	G06Q 20/401
2020/0066072	12/2019	Galvez	N/A	H04L 9/3239
2020/0097927	12/2019	Groarke	N/A	H04L 9/3239

2020/0125738	12/2019	Mahatwo	N/A	H04L 63/20
2020/0351074	12/2019	Wood	N/A	H04L 9/0861
2021/0097795	12/2020	Manchovski	N/A	H04L 63/108
2021/0304197	12/2020	Pomassl	N/A	N/A
2023/0313898	12/2022	Carpenter	137/512	F16L 41/03

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
10031993	12/2021	VN	B05D 7/14

OTHER PUBLICATIONS

Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” Decentralized business review (2008). cited by examiner
Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” Decentralized business review (2008). (Year: 2008). cited by examiner
Andreas Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Dec. 2014, O'Reilly Media First Edition (2014). cited by applicant

Primary Examiner: Cervetti; David Garcia

Attorney, Agent or Firm: KDW Firm PLLC

Background/Summary

RELATED APPLICATIONS (1) This application is a continuation of U.S. patent application Ser. No. 16/822,928, filed on Mar. 18, 2020, which is a continuation of U.S. patent application Ser. No. 16/230,106, filed on Dec. 21, 2018, (issued as U.S. Pat. No. 10,637,644), both applications titled “SYSTEM AND METHOD FOR AUTHORIZING TRANSACTIONS IN AN AUTHORIZED MEMBER NETWORK”. The contents of the aforementioned applications are incorporated herein by reference in their entireties.

BACKGROUND
(1) Although today's credit card transactions often take seconds or less to authorize, there are many parties involved in clearing the transaction. For example, credit card transactions frequently occur because of interactions between merchants, acquiring banks, credit card associations, credit card issuers and consumers.
(2) Credit card associations, such as Visa®, MasterCard® and American Express®, act as custodians and clearing houses for their respective card brand. The primary responsibilities of card associations include governing their members, establishing interchange fees and qualification guidelines, acting as the arbiter between issuing and acquiring banks, maintaining and improving the card network and making a profit.
(3) Acquiring banks, or “merchant banks” are registered members of card associations that contract with merchants to create and maintain merchant accounts that allow merchants to accept credit and debit cards. Acquiring banks deposit funds from credit card sales into a merchant's bank account. Payment gateways may also provide portals that route transactions to acquiring banks, for example through the use of online shopping carts and the like.
(4) Credit card issuers issue credit cards to consumers. Issuing banks pay acquiring banks for purchases that their cardholders make, and the cardholder is responsible for repaying the issuing bank under the terms of their credit card agreement.

(5) Card issuers, acquiring banks and payment gateways all level fees on either or both of the merchants and card members for each transaction. Therefore, while the current payment authorization network can quickly authorize consumer purchases, they are expensive. For example, there may be wholesale fees charged by credit card issuers and credit card associations. On top of the wholesale fees, merchants may incur credit card processing fees, payable to acquiring banks or payment gateways.

(6) It would be desirable to identify a system and method for quick, reliable processing of consumer transactions without the inherent expenses of current credit card processing systems.

SUMMARY

(7) According to one aspect of the invention, a method for authorizing transactions received from nodes of an authorized network of nodes at a Point-Of-Sale (POS) device of a merchant includes receiving a transaction from a node coupled to the POS device, the transaction including a request to modify a state of an account of the node. The state of the account of the node is preferably managed by a blockchain, and the transaction includes a blockchain update request comprising an account value and a transaction value. The method includes the steps of retrieving a blockchain copy from a memory of the POS device, comparing the account value of the blockchain update request to an account value of the blockchain copy, comparing the account value of the blockchain copy to the transaction value and in response to the steps of comparing, selectively authorizing the transaction by validating the blockchain update request. With such an arrangement, POS transactions can be quickly and reliably processed without incurring the expenses often inherent in managing centralized fiat currency.

(8) According to another aspect of the invention, a device for use by a merchant to authorize transactions received from a node is provided, where both the node and the device are members of an authorized network of nodes. At least a subset of nodes is associated with one or more accounts and the state of each account of each node is managed by a blockchain such that copies of each blockchain are maintained at each node of the authorized network. The device includes a storage device to store a first copy of a blockchain associated with an account of a node, a local interface to receive a transaction from the node, the transaction including a blockchain update request including a node identifier, an account value, and a transaction value and blockchain control logic. The blockchain control logic includes an authentication unit, coupled to the local interface, to authenticate the transaction request using the first copy of the blockchain and a validation unit to selectively authorize the transaction in response to the account value and the transaction value of the blockchain update request. The blockchain control logic also includes blockchain update logic, comprising a queue for storing a plurality of transactions received at the device and a network interface for periodically forwarding the plurality of transactions in bulk to a coupled central authentication server.

(9) According to a further aspect of the invention, a method for authorizing transactions received at a merchant device from a member node is provided. The member node and the merchant device are preferably members of an authorized network of nodes which manages at least one account of at least one node in the authorized network using a blockchain. The method includes the steps of receiving a transaction from a member node coupled to the merchant device including a request to modify a state of an account of the member node, wherein the state of the account of the member node is managed by a blockchain and the transaction includes a blockchain update request comprising an account value and a transaction value. The method includes the steps of retrieving a blockchain copy from a memory of the merchant device, selectively authorizing the transaction in response to the transaction and at least one of the copy of the blockchain and a received validation of the blockchain update from a different node in the authorized network of nodes and forwarding the blockchain update request to a central authorization server. In response to receipt of a validation from the different node, the method includes the steps of generating an updated block including the state of the account of the member node following the transaction, broadcasting the updated block

to the authorized network, appending the updated block to the copy of the blockchain; and storing the copy of the blockchain in the memory.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) FIG. **1** is a block diagram of one exemplary implementation of a transaction processing system according to aspects of the present invention;

(2) FIG. **2** is a block diagram of a second exemplary implementation of a transaction processing system according to aspects of the present invention;

(3) FIG. **3** is a flow diagram illustrating exemplary steps that may be performed to populate the authorized networks of FIG. **1** or FIG. **2** with blockchain account information;

(4) FIG. **4** is a flow diagram illustrating exemplary steps that may be performed during processing of transactions in either the system of FIG. **1** or the system of FIG. **2**;

(5) FIG. **5** is a flow diagram illustrating exemplary steps that may be performed by member devices of an authorized network of FIG. **1** or FIG. **2**;

(6) FIG. **6** illustrates exemplary components of a blockchain which may be used to support the process of FIG. **4**;

(7) FIG. **7** is a detailed illustration of a blockchain of FIG. **6**;

(8) FIG. **8** is a block diagram illustrating exemplary components of a merchant device of FIG. **1** or FIG. **2**; and

(9) FIG. **9** is a block diagram illustrating exemplary components that may be included in a member node of FIG. **1** or FIG. **2**.

DETAILED DESCRIPTION

(10) In a system that provides fast, reliable transaction processing, members of an authorized network manage account information using blockchain ledgers. An authorized network is a network of members which have been admitted to the network by a central authority. For example, a central authority may be a credit card issuer, bank, or other entity that manages typical fiat currency payment accounts for a consumer. Members of the authorized network include both consumers and merchants. Because both the consumer and the merchant maintain copies of the blockchain, for any consumer/merchant transaction, both entities can quickly validate the transaction because both are aware, via their blockchain entries, of the current status of the account sourcing the transaction. With such an arrangement, fast and accurate transaction validation can be provided without incurring the processing charges inherent in traditional fiat currency credit transactions.

(11) In one embodiment, the components that are used to support member blockchain transactions are provided in a transaction device having substantially a look and feel of a traditional credit card and including both memory and processing capability. In alternate embodiments, the components that are used to support member blockchain transactions are implemented using dedicated software operating on a smart device of the consumer. In either embodiment, members may maintain multiple accounts on a single member device, wherein each account may be associated with a different authorized network.

(12) These and other features of the invention will now be described with reference to the figures, wherein like reference numerals are used to refer to like elements throughout.

(13) As used in this application, the terms “system” and “component” are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, examples of which are described herein. For example, a component can be, but is not limited to being, a process running on a processor, a processor, a hard disk drive, multiple storage drives (of optical and/or magnetic storage medium), an object, an executable, a thread of

execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers.

(14) Further, components may be communicatively coupled to each other by various types of communications media to coordinate operations. The coordination may involve the uni-directional or bi-directional exchange of information. For instance, the components may communicate information in the form of signals communicated over the communications media. The information can be implemented as signals allocated to various signal lines. In such allocations, each message is a signal. Further embodiments, however, may alternatively employ data messages. Such data messages may be sent across various connections. Exemplary connections include parallel interfaces, serial interfaces, and bus interfaces.

(15) FIG. **1** is a block diagram illustrating several components that may be found in a transaction processing system **100** of the present invention. System **100** is shown to include a central authority **102** coupled via network **150** to one or more merchant devices **110**, **120** and **130**. Each merchant device **110**, **120** and **130** is communicatively coupled to one or more members devices. For example, the merchant device **110** is shown coupled to member devices **112**, **114** and **116**, the merchant device **120** is shown coupled to member devices **122**, **124** and **126**, the merchant device **130** is shown coupled to member devices **132**, **134** and **136**. For the purposes herein, the term 'communicatively coupled' means that each device includes communication and interface logic that enables the devices to exchange blockchain messages and other information. The logic may provide for either or both of direct coupling of the member device and the merchant (i.e., a card reader or the like), and/or may include logic for communicating over a network, such as a wireless or Bluetooth network.

(16) Member devices, in one embodiment, comprise portable transaction devices comprising memory and processing capabilities. In some embodiments, member devices may include credit-card like devices comprising memory and processing capabilities to support the functions described herein. In some embodiments, member devices may comprise so-called 'smart' cards, credit cards having embedded processors, cellular phones, tablet devices and the similar devices.

(17) Herein, an "authorized network" includes members and merchant devices that have been authorized by a central authority to access and modify an authorized account. The members and merchant devices communicate using blockchain messages that enable modification of an account according to a defined consensus protocol. Every member of an authorized network stores a blockchain for the authorized account. Thus, in the embodiment of FIG. **1**, merchant devices **110**, **120** and **130** as well as members **112**, **114**, **116**, **122**, **124**, **126**, **132**, **134** and **136** together form the authorized network for an account managed by blockchain **105**, and therefore each store a copy of blockchain **105**.

(18) FIG. **2** illustrates a second embodiment of a transaction system **200**, wherein members may be part of more than one authorized network, and concomitantly store blockchain copies for multiple authorized accounts. The authorized networks may include currency networks disclosed herein and cryptocurrency accounts, such as Bitcoin, Litecoin, Ethereum and the like. According to one aspect, members may have multiple authorized accounts. Multiple accounts may be managed by a single blockchain, separate accounts may be managed by separate blockchains, or some accounts may be managed by blockchains while others are managed using existing fiat-based account management systems. For example, while member **211** has only one authorized account for its own use (managed by blockchain **204**), it is shown to be a member of other authorized networks which manage accounts for members **212** and **213**. Member **212** may have a virtual wallet (a.k.a. "e-wallet") having access to multiple accounts, each account managed by a respective blockchain **205**, **206**. Member device **213** may have an e-wallet that provides access to three accounts, as managed by blockchains **207**, **208** and **209**. As described, each member of the authorized network stores

blockchain information for the authorized network account. Thus member **211**, in addition to storing the blockchain **204** for its own account, also stores copies of the blockchains **205** and **206** for member **212** accounts, and stores copies of blockchains **207**, **208** and **209** for member **213** accounts. Member **212** stores copies of blockchain **204** for member **211**'s account, as well as copies of blockchains **207**, **208** and **209** for member **213** accounts. In addition to blockchains **207**, **208** and **209**, member **213** stores copies of blockchains **204**, **205** and **206**, for member **211** and member **212**'s accounts. As such, each member can validate the transactions of other members in the authorized network.

(19) Merchant device **210** similarly stores blockchains for all accounts of all authorized networks which the merchant device is a member. Thus, the merchant device stores blockchains **204-209**, associated with member device accounts. The merchant device **210** also advantageously stores blockchains (such as blockchain **215**) for merchant accounts; i.e., merchant banks that receive the funds of the transaction. As with the central authority **202**, a merchant bank **225** associated with the merchant may include a copy of the merchant devices blockchain **215**. Such an arrangement allows the merchant device **210** to transact with the merchant bank **225** using processes and protocols substantially similar to those that occur between the member device **211** and the merchant device **210**.

(20) The central authority stores blockchains for all accounts that have been authorized by the central authority. Accordingly, central authority stores blockchains **204-209** that can be used as part of the validation of transactions by merchant **210**. In addition, the central authority may store other blockchains **215-219**, associated with other authorized accounts for other merchants (not shown).

(21) FIG. **3** illustrates exemplary steps that may be performed in one embodiment of a process **300** for initial setup of an authorized account that may be used to manage transactions according to principles of the present invention. At step **302** a member opens an account with a central authority, such as a bank, card issuer, cryptocurrency issuer or the like. At step **302** the central authority populates an initial blockchain block using information related to the account, such as a member number, an account number, and an account value. The central authority may also provide one or more of a public key and/or private key to the member, to be used to authenticate the member during a transaction.

(22) At steps **308** and **310**, the central authority distributes the blockchain to the merchant devices and the member devices. The blockchain is stored in the memory of the member device, together with any other blockchains of authorized networks, prior to physical delivery of the device to the member consumer. In some embodiments, a member device may also be hardcoded with the private key for the member.

(23) Once the blockchain is provided to the member, it may also be provided to the merchants that the member intends to transact with. Which merchant devices are selected to receive the blockchain may be determined in response to a variety of considerations, including whether the account is merchant specific (i.e., limited to use at a particular merchant, such as a store specific credit card), or a general-purpose account (i.e., may be used at a variety of merchants, such as a Visa card). For merchant specific cards, the central authority can distribute the blockchains for each member account to the specific merchants. The distribution may be geographically limited based on an address of the member, although this is not required.

(24) For general-purpose accounts, the particular merchants to forward the blockchains may be selected using predictive algorithms, for example based on historical or expected spending habits of the member. Alternatively, the blockchains may be broadcast to and stored by all merchants accepting payments from the particular card type.

(25) In alternate embodiments, the blockchain is delivered to the merchant by the central authority only following the first initial use of the member device at the merchant. It is understood that this initial population may result in incurred delay in an initial transaction, although the effect of this delay on the overall efficiency of the transactions is minimal. To overcome the problems associated

with initially populating merchant devices in this manner, a merchant may allow the member to ‘check in’ with their authorized network when they first arrive at the store or merchant website. During this check in, the member may communicably connect with the merchant device, forwarding account information and private/public key information to the merchant. The merchant may, in turn, forward this information to the central authority, which authenticates the member. Following authentication, the central authority may then populate the merchant's copy of the blockchain for the member's account. When the member is ready to perform a transaction, it may be quickly and reliably verified using the process of FIG. **4**.

(26) FIG. **4** illustrates exemplary steps that may be performed during a transaction process **400** by each of the member devices **211**, the merchant device **210** and central authority **202**. At step **402** the member device **211** communicably couples to the merchant device **210**, forwarding a blockchain message **405** including information associated with the desired transaction, including the resulting account balance and public/private key information. At step **403** the member device **211** awaits validation. At step **412**, the merchant device **210** authenticates the transaction by comparing the key received as part of the transaction against previously stored key information associated with the client, and at step **413** validates the blockchain transaction by first establishing that the blockchains are synchronized, and then establishing that the account balance represented in the merchant device's blockchain copy corresponds to the account balance as represented in the member devices blockchain message. By ‘synchronized’ it is meant that each of the devices stores the same information regarding the current status of the account.

(27) If it is determined at step **413** either that the blockchain copy at the merchant is not synchronized with the member account, or that there are insufficient funds in member's account, then at step **417** the merchant rejects the transaction, sending a rejection signal or other indication to the member device. The member device, receiving the rejection at step **403**, terminates the transaction.

(28) If, however, it is determined at step **413** that there are sufficient funds in a synchronized blockchain account, then at step **414** the merchant device **210** validates the transaction, sending a validation signal as part of a blockchain update **420** to the member device **211** and updating the blockchain to reflect the changes to member's account as a result of the transaction.

(29) At step **414** the merchant device initiates the process of updating the blockchain copies of other members and blockchain copies of the central authority. Because the member device and merchant device are both able to accurately validate blockchain transactions, it is realized that a network load advantage can be obtained without adversely affecting the accuracy of the transaction by bundling together blockchain updates and sending the transactions together in bulk to the central authority for processing. At step **416**, a merchant device taking advantage of this feature collects blockchain updates **415** and subsequently transmits the blockchain updates the central authority to enable it to update the blockchain copy.

(30) The number of blockchain updates which are bundled together is a matter of design choice, which may vary based on, inter alia, available memory and/or processing speed of the merchant device, the communication medium of network **250** and the loading at the central authority. In one embodiment, for example, ten blockchain updates may be forwarded in a bundle to the central authority, although the present invention is not limited to any particular number of bundled transactions.

(31) While the process of FIG. **4** describes a transaction between an authorized member device and an authorized merchant device, similar processes may be used to reliably and efficiently move funds between any two members of an authorized network, including member devices, merchant devices, central authorities, etc. The processing of the blockchain transaction as described in FIG. **4** may result in the generation of a new blockchain transaction by the merchant device **210** to transfer funds to merchant bank **225**.

(32) Referring now to FIG. **5**, a process **500** for updating blockchains of authorized members is

provided. At step **504**, as each member device communicates with the merchant device **210**, blockchain updates for all the accounts which the member device is an authorized member are received by the member device. This update process may occur as part of the transaction process of FIG. **4** when the member device is physically connected (for example inserted or swiped) at a merchant device. Alternatively, for smart member devices including wireless capability, the update process may occur over a wireless network when the member device is within transmit range of a transmitting member device of the authorized network.

(33) At step **506** the member device authenticates each received blockchain transaction. In one embodiment this may be done by determining whether the account balances, pre-transaction, are synchronized, and if so, at step **508** validating the blockchain update. In embodiments which seek to maintain the confidentiality of account information and values, blockchain contents may be hashed, and the authentication step may compare hashed values to validate transactions. Other methods of securing blockchain data or validating transactions may be substituted herein without affecting the scope of the invention.

(34) In one embodiment, the blockchain entries are validated by setting a ‘valid’ flag within a blockchain entry. Certain consensus protocols may require that a minimum number of members of the authorized network validate a first blockchain transaction prior to a member being able to perform a second transaction on the account.

(35) FIG. **6** depicts a logical model **600** of an exemplary blockchain **105**, consistent with disclosed embodiments. Such exemplary blockchains may comprise blocks, such as blocks **601***a*-**601***d*. Blocks may include messages, such as message **607***b* and message **607***d*. Generally, blocks may include a header, such as headers **603***a*-**603***d*, which uniquely identifies each block. The headers **603***a*-**603***d* may include a hash value generated by a hash function. A hash function is any function that can be used to map input data of arbitrary size to a hash value of a fixed size. For example, a header may include at least one of the previous block's hash value, a hash value generated based on any messages in the block (e.g., a Merkle root), and a timestamp. Consistent with disclosed embodiments, system **100** may require that blocks added to blockchain **105** satisfy at least one of a proof-of-work condition (e.g., a proof **605***a*-**605***d*) and a digital signature condition. It should be noted that although Proof-of-Work is described, other consensus mechanisms, such as Proof-of-Stake, Proof-of-Activity, or other messaging controls agreed to by the parties may be substituted here. For example, the headers **603***a*-**603***d* may include a nonce chosen to ensure the header satisfies the proof-of-work condition. As a non-limiting example, the proof-of-work condition may require the hash of the header fall within a predetermined range of values. As an additional example, the header may be digitally signed with a cryptographic key of an authorized system, and the digital signature may be included in the header. This digital signature may be verified using a key available to the members of system **100**. Generally, one or more designated nodes of an authorized member network (e.g., the member device or merchant device) may generate blocks **601** including headers **602**, proofs **605**, and messages **607** to initiate a payment transaction over the authorized network.

(36) FIG. **7** depicts a logical model of a message **607***b* stored in a blockchain (e.g., an element of blockchain **105**), consistent with disclosed embodiments. As will be described in more detail in FIGS. **8** and **9**, in some embodiments, a designated component of the system generates blockchain messages such as the message **607***b*. In some embodiments, message **607***b* may comprise index information **703**. In certain aspects, index information **703** may comprise information identifying a user. For example, index information **703** may be at least one of a full name, email address, phone number, or other non-sensitive personal information of the user. In various aspects, index information **703** may include one or more references to earlier blocks in the blockchain **105**. For example, index information **703** may include one or more references to one or more earlier blocks associated with the same user. A reference may include, as a non-limiting example, a hash of a preceding block in the blockchain associated with the same user. In some embodiments, index

information **703** may be obfuscated or encrypted according to methods known to one of skill in the art. For example, index information **703** may be encrypted with a cryptographic key. As an additional example, index information **703** may comprise a hash of the at least one of a full name, email address, phone number, or other non-sensitive personal information of the user.

(37) Message **607***b* may comprise a monetary transaction consistent with disclosed embodiments, including a transaction value.

(38) Cryptographic keys may be used to encrypt elements of messages in blocks, consistent with disclosed embodiments. Cryptographic keys may be associated with members of the system **100** (e.g., merchant devices, member devices, central authorities). In various aspects, at least some of the cryptographic keys may be associated with authorized systems. Corresponding cryptographic keys may be available to decrypt the encrypted message elements, consistent with disclosed embodiments. For example, when an element of a message in a block is encrypted with a symmetric key, the same symmetric key may be available for decrypting the encrypted element. As another example, when an element of a message in a block is encrypted with a private key, a corresponding public key may be available for decrypting the encrypted element and the corresponding cryptographic keys may be available to members of the authentication system.

(39) FIG. **8** illustrates exemplary components that may be included in a merchant device **800**, for example, a Point-Of-Sale (POS) device such as a card reader. The merchant device **800** includes a member interface **810** for exchanging transactions with authorized members and a credit authority interface **850** for updating blockchain copies maintained, for example, by the card issuer. A blockchain controller **820** may be a processor optimized to perform blockchain transactions using the protocols described herein. For example, the blockchain controller may be programmed to authenticate the members using the private and public keys, to extract account information, such as account balances and account owner, and to extract transaction information such as a transaction amount. The blockchain controller may also be programmed to validate a blockchain transaction in response to key data, transaction amounts and account balances. Interface **850** is shown to include a data queue **830** of blockchain entries, collected as described with regard to FIG. **4** prior to bulk transfer of the entries to the appropriate central authority.

(40) FIG. **9** illustrates exemplary components that may be included in a member device **900** according to aspects of the invention. The member device **900** includes a merchant interface **950**, a transaction controller **902**, and a blockchain controller **904**. The member device further may comprise a storage device **920**, that may be used to store both authentication information, such as public key **922** and private key **924**, and one or more blockchains such as blockchains **925***a* and **925***b*. According to one aspect, transaction device **900** may also include a Field Programming Gate Array (FPGA) which may be optimized prior to or during currency transactions for improved performance of the currency operations of the transaction device as described in U.S. patent application Ser. No. 16/230,106 entitled “A SYSTEM AND METHOD FOR OPTIMIZING CRYPTOCURRENCY TRANSACTIONS” filed on even date herewith and incorporated by reference.

(41) Although two blockchains **925***a*, **925***b* are shown, it is appreciated that the number of blockchains maintained by a transaction device **900** will vary depending upon the number of currency accounts available to a user of the transaction device. Each blockchain may be associated with the same or different currency accounts. The currency accounts may be associated with the same or different currency networks. For example, it is contemplated that a transaction device may store blockchains for fiat currency networks using the consensus protocols described herein, and may also store blockchains for cryptocurrency accounts including, but not limited to, cryptocurrency networks such as Bitcoin, Ethereum, PeerCoin, LiteCoin and the many variants thereof.

(42) In one embodiment, the transaction controller **902** forwards information regarding a transaction, including a transaction amount and a transaction account (i.e., the sourcing account for

the transaction) to the blockchain controller. The transaction information may be received from the member operating the device or from the merchant, from the merchant, or some combination thereof. For example, when the member device is a smart card, the member may interface with a POS using a keypad; wherein after ringing up a sale the member is asked to authorize a transaction of a given amount. In some embodiments, the member may also be prompted to specify which of the e-wallet type accounts of the card should be used to source the transaction.

(43) Upon approval of the transaction, the transaction controller forwards the account information and transaction value to the blockchain controller **904**. The blockchain controller uses this information to build a block such as block **601***a* shown in FIG. **6**. Thus, the blockchain controller **904** includes logic to build a header, nonce, and proof of work, or to otherwise provide authentication attributes according to an agreed-upon blockchain protocol. The resultant block **906** is forwarded to the merchant interface **950**. As described above, one or more fields of the block may be encoded using the public key **922**, private key **924** or some combination thereof for authentication and security purposes. Following validation, as described above, the blockchain update **906** may be added to blockchain **925**. Memory **920** is also coupled to receive and store blockchain updates for authorized member device accounts.

(44) Although FIG. **9** describes components that may be included on a smart card, the transaction processing protocol and method is not limited to use with smart cards. Alternative implementations of FIG. **9** using functionality provided by a smartphone or other intelligent device may also be used, and thus the present invention is not limited to any particular implementation of member devices, merchant devices or central authority structures.

(45) Accordingly, a system and method have been described that enables fast, accurate merchant transactions with fewer intermediaries and concomitant costs. Some embodiments may be described using the expression “one embodiment” or “an embodiment” along with their derivatives. These terms mean that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment. Moreover, unless otherwise noted the features described above are recognized to be usable together in any combination. Thus, any features discussed separately may be employed in combination with each other unless it is noted that the features are incompatible with each other.

(46) With general reference to notations and nomenclature used herein, the detailed descriptions herein may be presented in terms of functional blocks or units that might be implemented as program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art.

(47) A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

(48) Further, the manipulations performed are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein, which form part of one or more embodiments. Rather, the operations are machine operations. Useful machines for performing operations of various embodiments include general purpose digital computers or similar devices.

(49) Some embodiments may be described using the expression “coupled” and “connected” along with their derivatives. These terms are not necessarily intended as synonyms for each other. For example, some embodiments may be described using the terms “connected” and/or “coupled” to indicate that two or more elements are in direct physical or electrical contact with each other. The term “coupled,” however, may also mean that two or more elements are not in direct contact with each other, but still co-operate or interact with each other.

(50) Various embodiments also relate to apparatus or systems for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a general-purpose computer as selectively activated or reconfigured by a computer program stored in the computer. The procedures presented herein are not inherently related to a particular computer or other apparatus. Various general-purpose machines may be used with programs written in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given.

(51) It is emphasized that the Abstract of the Disclosure is provided to allow a reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, various features are grouped together in a single embodiment to streamline the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. In the appended claims, the terms “including” and “in which” are used as the plain-English equivalents of the respective terms “comprising” and “wherein,” respectively. Moreover, the terms “first,” “second,” “third,” and so forth, are used merely as labels, and are not intended to impose numerical requirements on their objects.

(52) What has been described above includes examples of the disclosed architecture. It is, of course, not possible to describe every conceivable combination of components and/or methodologies, but one of ordinary skill in the art may recognize that many further combinations and permutations are possible. Accordingly, the novel architecture is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims.

Claims

1. A computer-implemented method, comprising: communicatively coupling, by a member device, to a merchant device of a plurality of merchant devices of an authorized network of nodes, wherein the authorized network of nodes comprises a plurality of member devices and the plurality of merchant devices, wherein each of the nodes is associated with at least one account, and a state of each account of each node is managed by a blockchain such that copies of the blockchain are maintained by at least a portion of the plurality of member devices and the plurality of merchant devices; receiving, by the member device, blockchain updates for all accounts of which the member device is an authorized member; determining, by the member device, whether account balances for each of the accounts in the blockchain updates are synchronized; sending, by the member device, a transaction request to the merchant device, the transaction request including a blockchain message including a key, an account balance of an account associated with the member device and maintained in a first copy of the blockchain on the member device, and a transaction value; receiving, by the member device, a rejection indication or a validation indication from the merchant device; halting a transaction associated with the transaction request in response to reception of the rejection indication; updating the first copy of the blockchain based on the

transaction associated with the transaction request in response to reception of the validation indication from the merchant device.

2. The computer-implemented method of claim 1 wherein receiving the validation indication is in response to verification that each copy of the blockchain is synchronized, and that an account balance in a blockchain copy associated with the merchant device corresponds to the account balance in the blockchain message; and wherein receiving, by the member device, the blockchain updates for all the accounts of which the member device is an authorized member is performed as part of a transaction process in response to the member device being inserted into, swiped, or tapped at the merchant device, but before the transaction request is sent to the merchant device.

3. The computer-implemented method of claim 1, wherein receiving the rejection indication is in response to the blockchain not being synchronized between the member device and the merchant device or there are insufficient funds in an account associated with the member device.

4. The computer-implemented method of claim 1, wherein each of the plurality of member devices comprises one of a portable transaction device, a smart card, a credit card, a mobile device, a cellular device, or a tablet device.

5. The computer-implemented method of claim 1, wherein the member device comprises a virtual wallet to access one or more accounts, including the account, and each account is associated with a different blockchain.

6. The computer-implemented method of claim 1, comprising: receiving, by the member device, the first copy of the blockchain from a central authority; and storing, by the member device, the first copy of the blockchain in a memory, wherein the memory is to store one or more blockchains of the authorized network of nodes, including the blockchain.

7. The computer-implemented method of claim 6, wherein the member device receives the first copy of the blockchain from the central authority in response to an initial transaction with the merchant device.

8. The computer-implemented method of claim 1, comprising periodically communicating, by the member device, with the merchant device to update the first copy of the blockchain.

9. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to: communicatively couple to a merchant device of a plurality of merchant devices of an authorized network of nodes, wherein the authorized network of nodes comprises a plurality of member devices and the plurality of merchant devices, wherein each of the nodes is associated with at least one account, and a state of each account of each node is managed by a blockchain such that copies of the blockchain are maintained by at least a portion of the plurality of member devices and the plurality of merchant devices; receive, by the processor, blockchain updates for all accounts of which the processor is an authorized member; determining, by the processor, whether account balances for each of the accounts in the blockchain updates are synchronized; send a transaction request to the merchant device, the transaction request including a blockchain message including a key, an account balance of an account associated with a member device of the plurality of member devices and maintained in a first copy of the blockchain on the member device, and a transaction value; receive a rejection indication or a validation indication from the merchant device; halt a transaction associated with the transaction request in response to reception of the rejection indication; update the first copy of the blockchain based on the transaction associated with the transaction request in response to reception of the validation indication from the merchant device.

10. The computer-readable storage medium of claim 9, wherein receiving the validation indication is in response to verification that each copy of the blockchain is synchronized, and that an account balance in a blockchain copy associated with the merchant device corresponds to the account balance in the blockchain message; and wherein receiving, by the processor, the blockchain updates for all the accounts of which the processor is an authorized member is performed as part of a transaction process in response to the member device being inserted into, swiped, or tapped at the

merchant device, but before the transaction request is sent to the merchant device.

11. The computer-readable storage medium of claim 9, wherein receiving the rejection indication is in response to the blockchain not being synchronized between the member device and the merchant device or there are insufficient funds in an account associated with the member device.

12. The computer-readable storage medium of claim 9, wherein each of the plurality of member devices comprises one of a portable transaction device, a smart card, a credit card, a mobile device, a cellular device, or a tablet device.

13. The computer-readable storage medium of claim 9, wherein the member device comprises a virtual wallet to access one or more accounts, including the account, and each account is associated with a different blockchain.

14. The computer-readable storage medium of claim 9, comprising further instructions to cause the processor to: receive and process the first copy of the blockchain from a central authority; and store the first copy of the blockchain in a memory, wherein the memory is to store one or more blockchains of the authorized network of nodes, including the blockchain.

15. The computer-readable storage medium of claim 14, wherein the member device receives the first copy of the blockchain from the central authority in response to an initial transaction with the merchant device.

16. The computer-readable storage medium of claim 9, comprising further instructions to cause the processor to periodically communicate with the merchant device to update the first copy of the blockchain.

17. A member device comprising: a processor; and a memory storing instructions that, when executed by the processor, cause the processor to: communicatively couple to a merchant device of a plurality of merchant devices of an authorized network of nodes, wherein the authorized network of nodes comprises a plurality of member devices and the plurality of merchant devices, wherein each of the nodes is associated with at least one account, and a state of each account of each node is managed by a blockchain such that copies of the blockchain are maintained by at least a portion of the plurality of member devices and the plurality of merchant devices; receive, by the member device, blockchain updates for all accounts of which the member device is an authorized member; determine, by the member device, whether account balances for each of the accounts in the blockchain updates are synchronized; send a transaction request to the merchant device, the transaction request including a blockchain message including a key, an account balance of an account associated with the member device and maintained in a first copy of the blockchain on the member device, and a transaction value; receive a rejection indication or a validation indication from the merchant device; halt a transaction associated with the transaction request in response to reception of the rejection indication; update the first copy of the blockchain based on the transaction associated with the transaction request in response to reception of the validation indication from the merchant device.

18. The member device of claim 17 wherein receiving the validation indication is in response to verification that each copy of the blockchain is synchronized, and that an account balance in a blockchain copy associated with the merchant device corresponds to the account balance in the blockchain message; and wherein receiving, by the member device, the blockchain updates for all the accounts of which the member device is an authorized member is performed as part of a transaction process in response to the member device being inserted into, swiped, or tapped at the merchant device, but before the transaction request is sent to the merchant device.

19. The member device of claim 17, wherein receiving the rejection indication is in response to the blockchain not being synchronized between the member device and the merchant device or there are insufficient funds in an account associated with the member device.

20. The member device of claim 17, wherein each of the plurality of member devices comprises one of a portable transaction device, a smart card, a credit card, a mobile device, a cellular device, or a tablet device.