US011176538B2

(12) **United States Patent**
Wyatt

(10) **Patent No.: US 11,176,538 B2**
(45) **Date of Patent: Nov. 16, 2021**

(54) **MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE**

(71) Applicant: **Virtual Electric Inc.**, San Jose, CA (US)

(72) Inventor: **David Wyatt**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **17/075,637**

(22) Filed: **Oct. 20, 2020**

(65) **Prior Publication Data**

US 2021/0304187 A1 Sep. 30, 2021

Related U.S. Application Data

(60) Continuation of application No. 16/459,150, filed on Jul. 1, 2019, now Pat. No. 10,810,579, which is a (Continued)

(51) **Int. Cl.**
G06Q 20/34 (2012.01)
G07F 19/00 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06Q 20/341*** (2013.01); ***G06K 19/06206*** (2013.01); ***G06K 19/0716*** (2013.01); ***G06K 19/07749*** (2013.01); ***G06Q 20/06*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/223*** (2013.01); ***G06Q 20/24*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06Q 20/341; G06Q 20/4012; G06Q 20/3827; G06Q 20/346; G06Q 20/065; G06Q 20/409; G06Q 20/352; G06Q 20/24; G06Q 20/385; G06Q 20/347; G06Q 20/223; G06Q 20/06; G06K 19/07749; G06K 19/0716; G06K 19/06206; G07F 7/0873; G07F 19/00
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

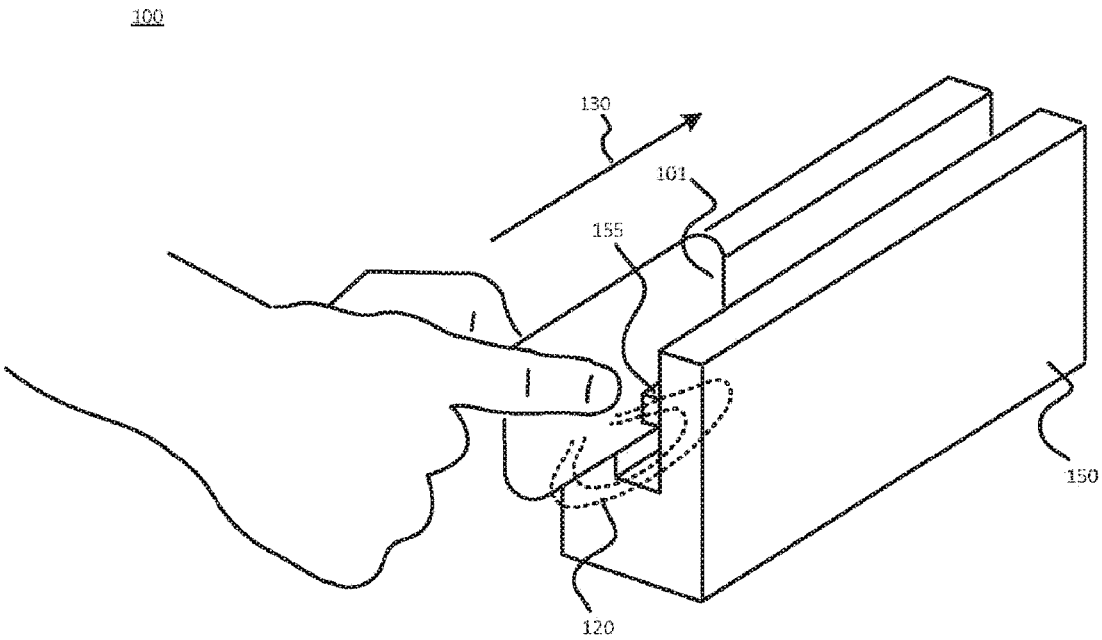
7,580,898 B2 * 8/2009 Brown G06Q 20/341 705/50
7,793,851 B2 * 9/2010 Mullen G06Q 20/40 235/493
(Continued)

Primary Examiner — Seung H Lee

(57) **ABSTRACT**

An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow the device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of the device for the purpose of authorizing or controlling use of the device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore the device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

30 Claims, 7 Drawing Sheets



Related U.S. Application Data

continuation of application No. 15/701,261, filed on Sep. 11, 2017, now Pat. No. 10,339,520, which is a continuation of application No. 14/981,757, filed on Dec. 28, 2015, now Pat. No. 9,760,884, which is a continuation of application No. 14/680,979, filed on Apr. 7, 2015, now Pat. No. 9,224,083, which is a division of application No. 14/217,261, filed on Mar. 17, 2014, now Pat. No. 9,022,286.

(60) Provisional application No. 61/794,891, filed on Mar. 15, 2013.

(51) **Int. Cl.**

G06Q 20/06	(2012.01)
G06Q 20/22	(2012.01)
G06Q 20/38	(2012.01)
G07F 7/08	(2006.01)
G06K 19/06	(2006.01)
G06K 19/07	(2006.01)
G06K 19/077	(2006.01)
G06Q 20/24	(2012.01)
G06Q 20/40	(2012.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/346*** (2013.01); ***G06Q 20/347*** (2013.01); ***G06Q 20/352*** (2013.01); ***G06Q 20/385*** (2013.01); ***G06Q 20/3827*** (2013.01); ***G06Q 20/409*** (2013.01); ***G06Q 20/4012*** (2013.01); ***G07F 7/0873*** (2013.01); ***G07F 19/00*** (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,851,370	B2	10/2014	DiMuro	
9,646,301	B2	5/2017	DiMuro	
9,928,496	B2 *	3/2018	Lee	G06Q 20/353
10,339,520	B2 *	7/2019	Wyatt	G06Q 20/346

* cited by examiner

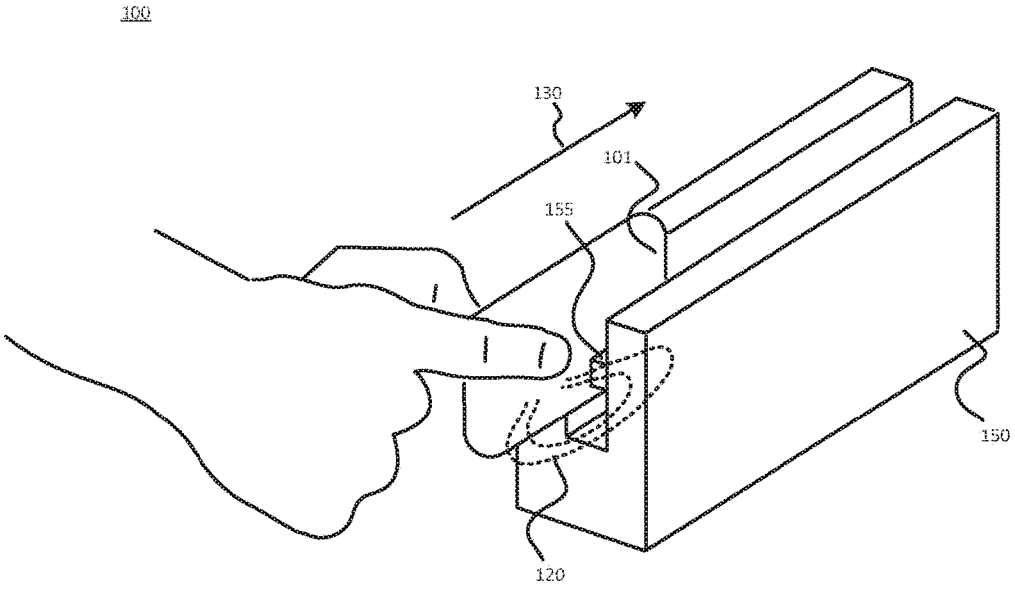


FIG. 1

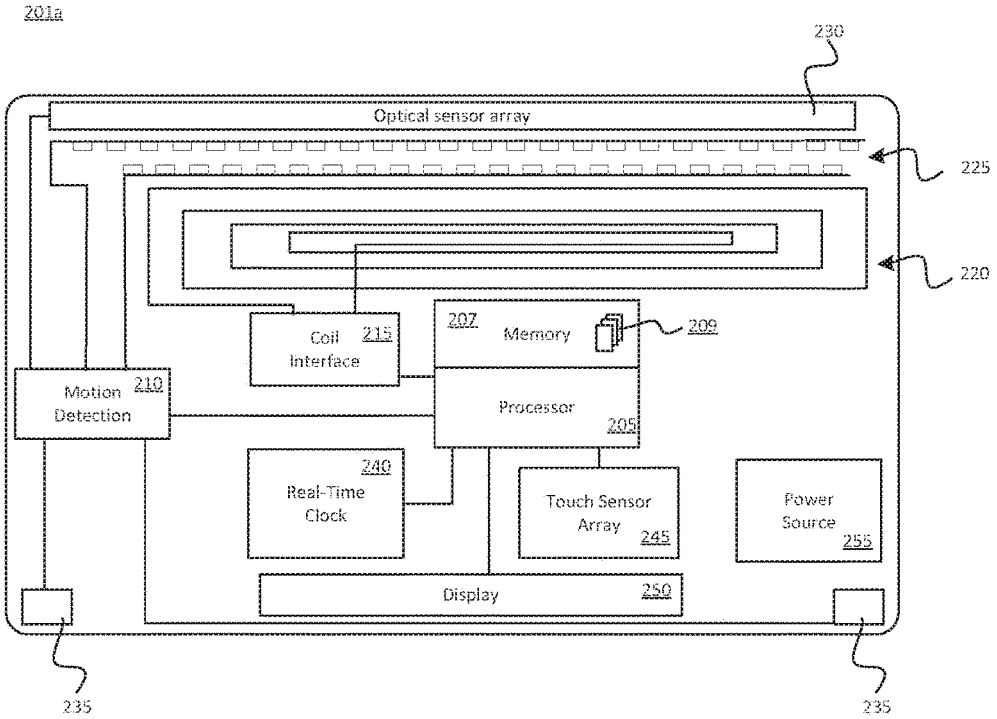

201a
230
Optical sensor array
225
220
Coil Interface 215
207
Memory
209
Motion Detection 210
Processor
205
240
Real-Time Clock
Touch Sensor Array 245
Power Source 255
Display 250
235
235

FIG. 2A

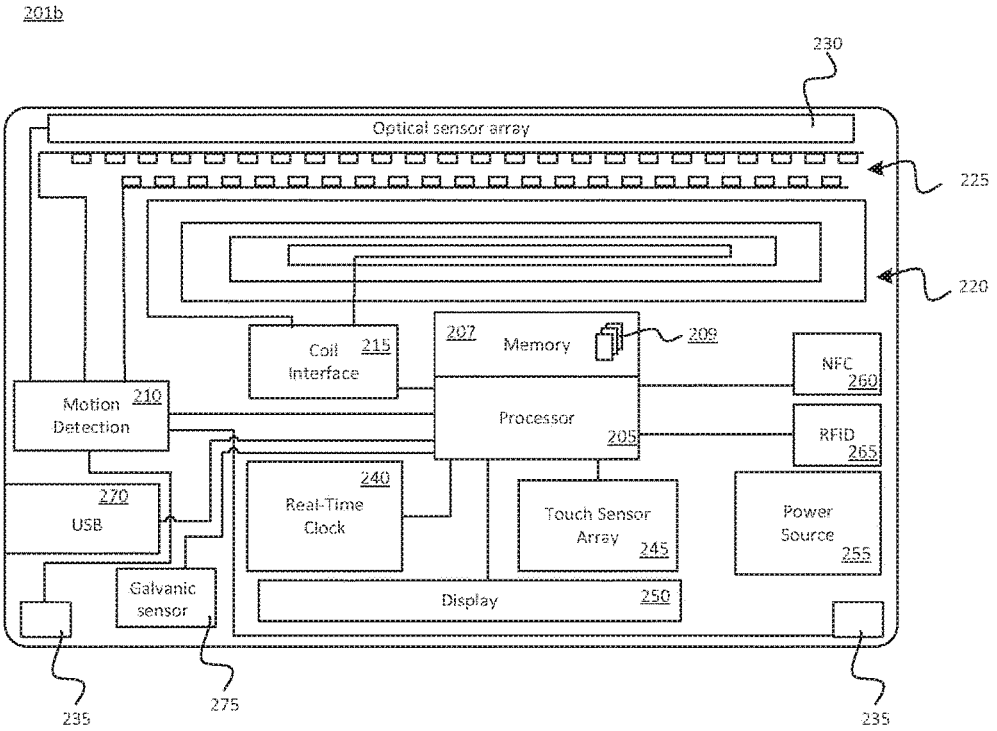

201b
230
Optical sensor array
225
220
Coil Interface 215
207
Memory
208
NFC 260
Motion Detection 210
Processor
205
RFID 265
270
USB
240
Real-Time Clock
Touch Sensor Array 245
Power Source 255
Galvanic sensor
Display 250
235
275
235

FIG. 2B

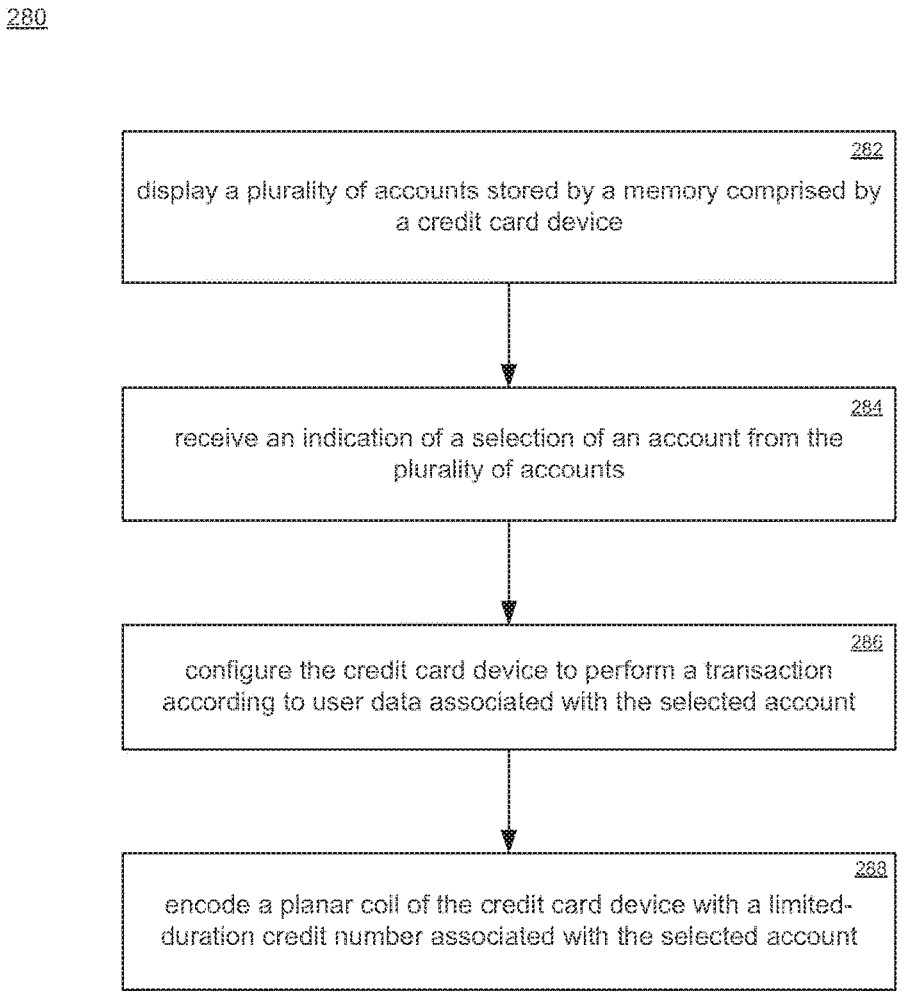

280
282
display a plurality of accounts stored by a memory comprised by a credit card device
284
receive an indication of a selection of an account from the plurality of accounts
286
configure the credit card device to perform a transaction according to user data associated with the selected account
288
encode a planar coil of the credit card device with a limited-duration credit number associated with the selected account

FIG. 2C

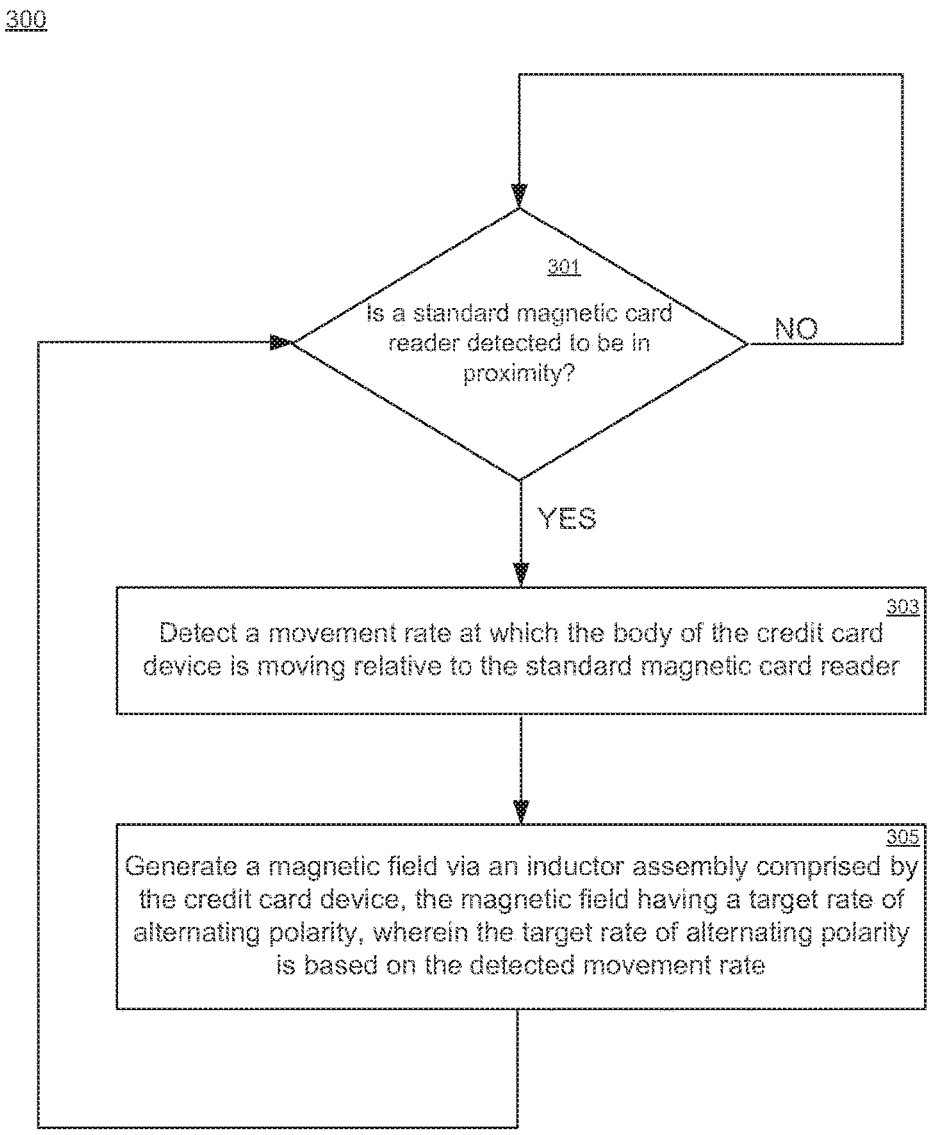

300
301
Is a standard magnetic card reader detected to be in proximity?
NO
YES
303
Detect a movement rate at which the body of the credit card device is moving relative to the standard magnetic card reader
305
Generate a magnetic field via an inductor assembly comprised by the credit card device, the magnetic field having a target rate of alternating polarity, wherein the target rate of alternating polarity is based on the detected movement rate

FIG. 3

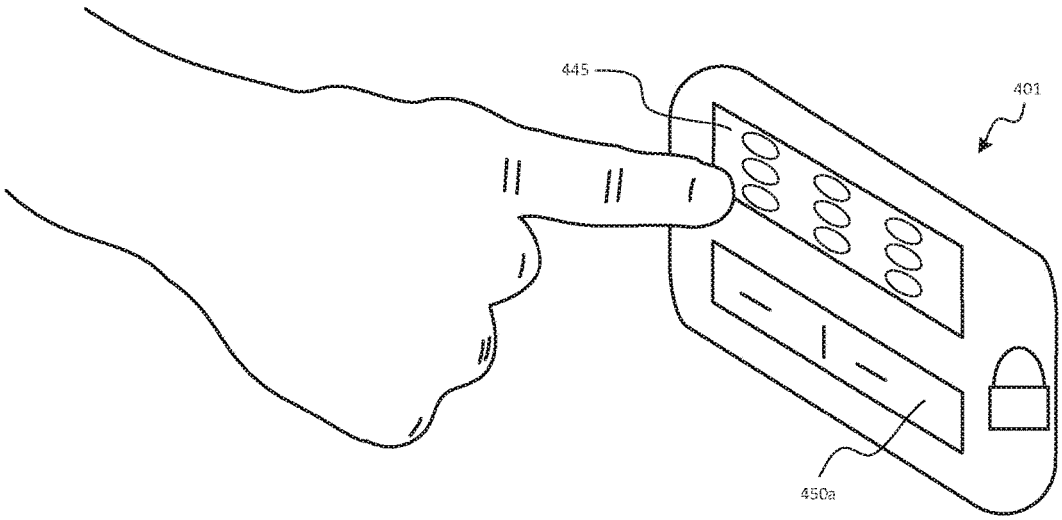


FIG. 4A

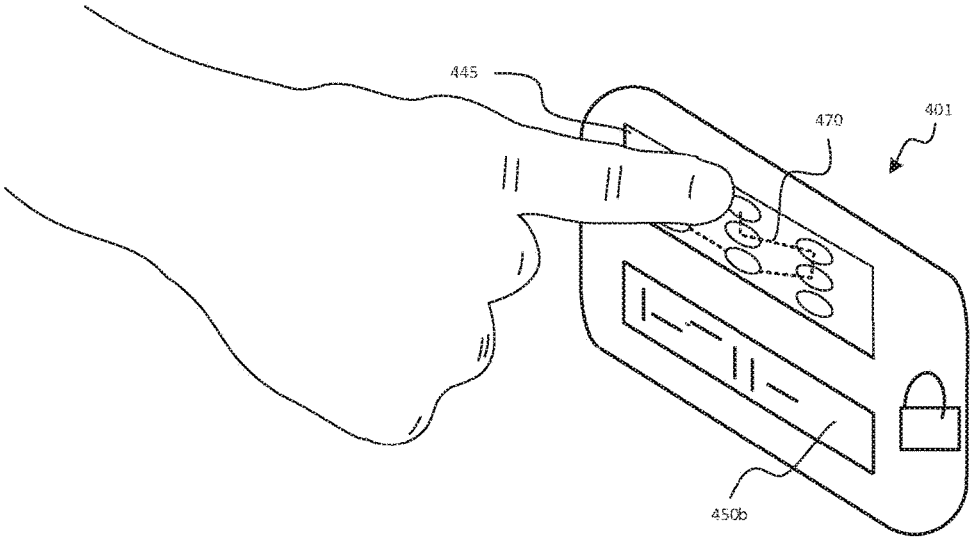


FIG. 4B

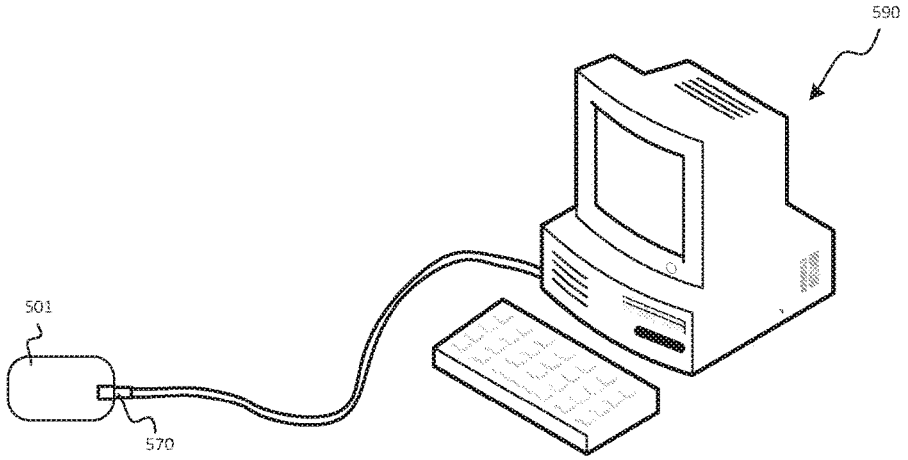


FIG. 5

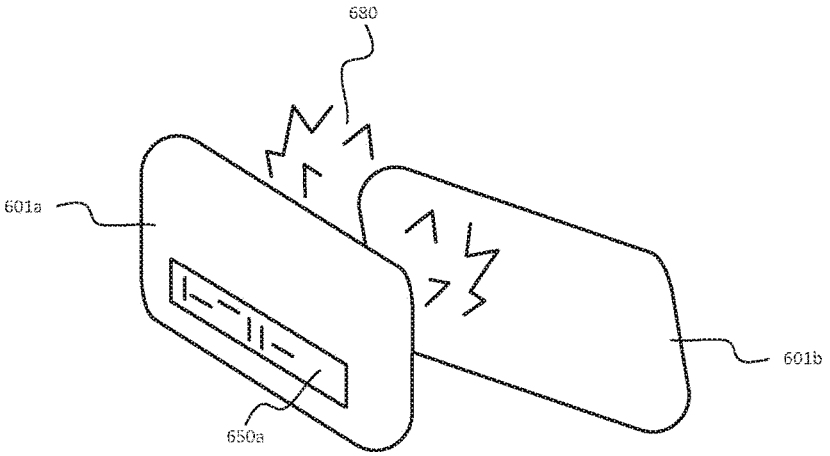


FIG. 6

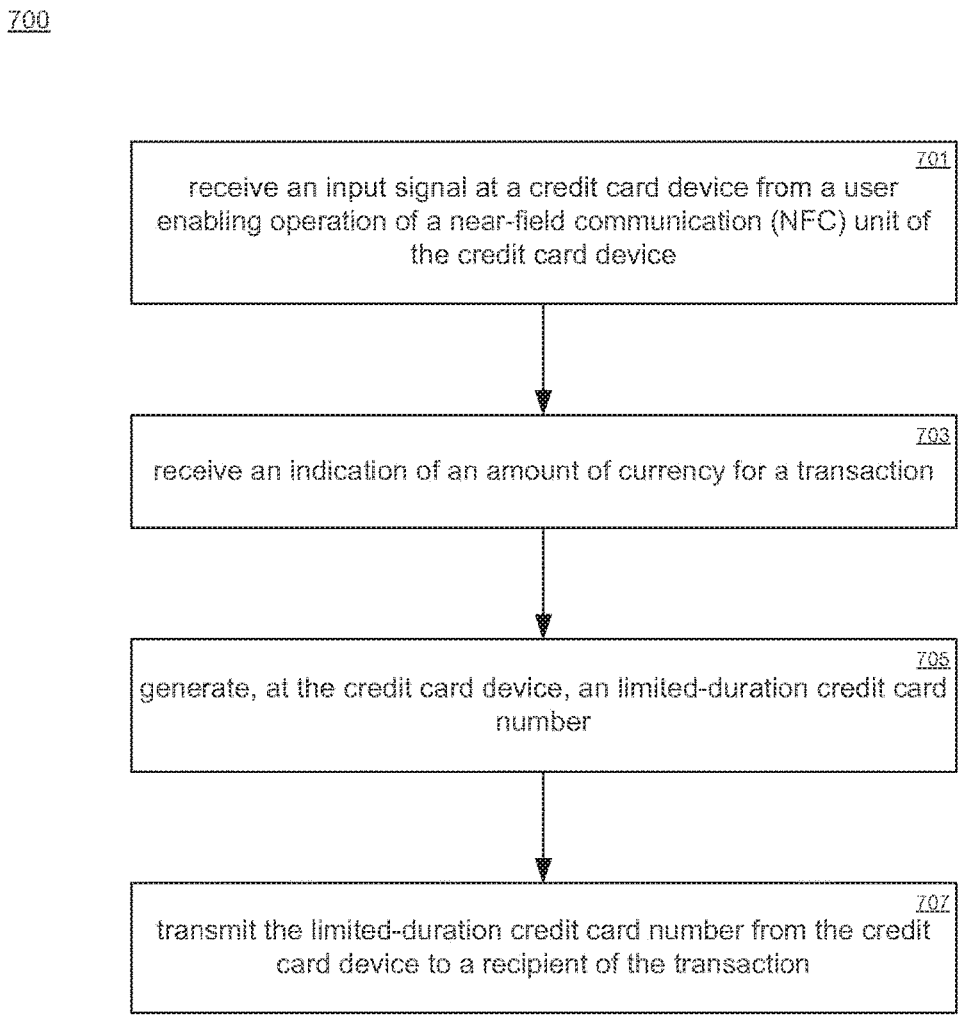

700
701
receive an input signal at a credit card device from a user enabling operation of a near-field communication (NFC) unit of the credit card device
703
receive an indication of an amount of currency for a transaction
705
generate, at the credit card device, an limited-duration credit card number
707
transmit the limited-duration credit card number from the credit card device to a recipient of the transaction

FIG. 7

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

RELATED APPLICATIONS

This is a Continuation application of commonly-owned U.S. patent application Ser. No. 16/459,150, now U.S. Pat. No. 10,810,579, filed Jul. 1, 2019, which in turn was a Continuation application of commonly-owned U.S. patent application Ser. No. 15/701,261, now U.S. Pat. No. 10,339,520, filed Sep. 11, 2017, which in turn was a Continuation application U.S. patent application Ser. No. 14/981,757, filed Dec. 28, 2015, now U.S. Pat. No. 9,760,884, which in turn was a continuation of U.S. patent application Ser. No. 14/680,979, filed Apr. 7, 2015, now U.S. Pat. No. 9,224,083, which in turn was a Division of U.S. patent application Ser. No. 14/217,261, filed Mar. 17, 2014, now U.S. Pat. No. 9,022,286, which in turn claims priority from Provisional Application 61/794,891, filed Mar. 15, 2013, each of which are hereby incorporated herein in their entirety by reference.

FIELD OF THE INVENTION

Embodiments according to the present disclosure generally relate to electronic or smart payment devices and, more specifically, to more secure, smart multi-function smart tokenizing electronic payment devices and transaction processing thereof.

BACKGROUND OF THE INVENTION

There are several different types of credit cards available in the marketplace at present. A first type of credit card is a conventional, standard piece of plastic with a magnetic strip, which is readily available and in wide commercial use. The advantage of this first type of credit card is that a large portion of the infrastructure for credit card transactions is built around this type of card, and consequently such a card works in a wide array of vendors' credit card machines, automated teller machines (ATMs), and other devices that support the present credit card and banking infrastructure.

Another type of credit card device employs the use of a smart integrated circuit chip. These types of credit cards have a built-in microprocessor with cryptographic capabilities. These microprocessors operate in a similar manner to a cell phone having a chip comprising a cryptographic processor. Such a smart card device requires contact with a reader in order to be read and to perform a transaction. The reader provides the manner in which a facility interacts with the built-in processor on the card, e.g., for purposes of performing verification on the authenticity of the card or for making a direct deposit on the card. These credit card devices also comprise a magnetic strip such that they are compatible with standard plastic credit card readers in wide use.

A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

A concern with each of these types of credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise. Therefore, these types of credit cards have security limitations. Further, cards employing smart integrated circuit

chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.

SUMMARY OF THE INVENTION

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow said device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of said device for the purpose of authorizing or controlling use of said device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore, said device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

More specifically, an aspect of the present disclosure provides an apparatus comprising: a thin card shaped sized body; a memory operative to store a plurality of identification data; a processor coupled to the memory; a user interface for selecting a select identification data of said plurality of identification data; a magnetic card reader detection unit for determining if the body is adjacent to a standard magnetic card reader; and an inductor assembly coupled to the processor and integrated into the body, the inductor assembly under processor control for generating a magnetic field of alternating polarity responsive to the body being detected as adjacent to a standard magnetic card reader, the magnetic field generated in a region substantially encompassing the standard magnetic card reader, wherein the magnetic field encodes said select identification data, and wherein the magnetic field is operable to be read by a magnetic read head of the standard magnetic card reader.

According to another aspect of the present disclosure, a multi-function electronic device comprises: a near-field communication (NFC) unit; a touch sensor array; a display; a motion rate detection array; a memory, storing a user data and a currency amount; and a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory; and wherein the processor initiates a device-to-device transaction between two devices by a detected proximity of a first device and a second device and an input of information by a first user via said touch sensor array, and wherein the device-to-device transaction comprises an exchange of stored currency and said user data between the first device and the second device via the NFC unit.

According to yet another aspect of the present disclosure, a method of performing a transaction comprises: receiving an input signal at a multi-function electronic device from a user enabling operation of a near-field communication (NFC) unit of the device; receiving an indication of an

amount of currency for a transaction; generating at said device a limited-duration payment number; and transmitting said limited-duration payment number from said device to a recipient of the transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present disclosure are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements.

FIG. **1** is an illustration depicting an exemplary interaction between a device and a standard magnetic card reader, according to an embodiment of the present disclosure.

FIGS. **2**A-**2**B are block diagrams illustrating data flow between the magnetic coils on the device and the microprocessor on the device according to an embodiment of the present disclosure.

FIG. **2**C depicts an exemplary process of selecting an account from a plurality of stored accounts according to an embodiment of the present disclosure.

FIG. **3** is a flowchart illustrating an exemplary process of generating a magnetic field with an alternating polarity according to an embodiment of the present disclosure.

FIGS. **4**A-**4**B illustrate a user interacting with a touch sensor of a device, according to an embodiment of the present disclosure.

FIG. **5** is an illustration of a device connected with a computing system and operating according to an embodiment of the present disclosure.

FIG. **6** is an illustration of two devices performing a transaction according to an embodiment of the present disclosure.

FIG. **7** depicts an exemplary process according to an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

Reference will now be made in detail to the various embodiments of the present disclosure, examples of which are illustrated in the accompanying drawings. While described in conjunction with these embodiments, it will be understood that they are not intended to limit the disclosure to these embodiments. On the contrary, the disclosure is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the disclosure as defined by the appended claims. Furthermore, in the following detailed description of the present disclosure, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. However, it will be understood that the present disclosure may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present disclosure.

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer generated step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven 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 borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present claimed subject matter, discussions utilizing terms such as "storing," "creating," "protecting," "receiving," "encrypting," "decrypting," "destroying," or the like, refer to the action and processes of a computer system or integrated circuit, or similar electronic computing device, including an embedded system, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Encoding Via an Alternating Polarity of a Magnetic Field

In one embodiment of the present disclosure, a smart multi-function electronic device comprises a dynamic magnetic region (strip) incorporating a main inductor assembly from which programmed magnetic field data symbols are dynamically generated. In one embodiment the inductor assembly may be a planar coil formed within the material that embodies the multi-function electronic device. An advantage of using a planar coil is that it can dynamically produce a magnetic field in such a manner as to emulate the interaction between a traditional magnetic strip and a conventional card reader. As the magnetic strip of a conventional card is passed through a magnetic reader head, stripes of alternating magnetic polarity embedded in the strip induce a magnetic field of alternating polarity at the reader head. The pattern formed by the alternating polarity of the magnetic field encodes information, which when transformed by a transducer to a current signal in the magnetic reader head, provides user information for a transaction.

Embodiments of the present disclosure provide a multi-function electronic device able to generate a programmed magnetic field, wherein data is encoded and represented by an alternating polarity of the generated magnetic field. In a similar manner to a conventional plastic card, the magnetic field produced by the planar coil is able to be read by a pickup (or "transducer") and to thereby transmit information to the magnetic card reader. FIG. **1** illustrates a payment transaction **100** performed between a multi-function electronic device **101** and a conventional magnetic reader **150**. The multi-function electronic device **101** generates a magnetic field of alternating polarity **120** to be read by the conventional magnetic card reader **150**, according to an embodiment of the present disclosure. The multi-function electronic device **101** is moved at a rate **130** relative to a magnetic reader head **155** of conventional magnetic card reader **150**. The magnetic field **120** extends with sufficient distance and intensity from **101** so as to be read by magnetic head reader **155**. The magnetic head reader **155** responds to the magnetic field **120** by producing a current in the conventional fashion, which is then interpreted as encoded information by the magnetic reader **150**. Therefore the magnetic field of alternating polarity **120** produced by the

multi-function electronic device **101** has a substantially identical encoding effect as a traditional magnetic strip.

A characteristic of encoding information in a conventional magnetic card strip is that binary information is encoded by the pattern of alternating magnetic polarity formed by ferromagnetic stripes embedded on the magnetic strip. As the conventional magnetic card strip has a standardized format, the encoding of information is provided at a specified data density (bits per inch), according to which conventional magnetic readers are designed for interpretation of encoded data. In order to most ably emulate a conventional card interaction with a conventional magnetic reader the multi-function electronic device **101** of the present disclosure is provided with a means of determining a substantially optimal rate for alternating the polarity of the generated magnetic field **120** in order to produce data at a rate which is able to be readily received and correctly interpreted by the conventional magnetic reader **150**. Embodiments of the present disclosure provide several means of determining the relative movement rate **130** between the multi-function electronic device **101** and the magnetic reader head **155**. These features, as well as other characteristics of the multi-function electronic device of the present disclosure, can be better appreciated by a description of the internal components and functions of multi-function electronic device **101**.

FIGS. **2**A and **2**B depict exemplary embodiments of a smart multi-function electronic device, in a block diagram view. The components of the block diagram are illustrated according to functional connections, and their locations should not be construed as being limited to the respective locations as depicted in FIGS. **2**A-**2**B. In FIG. **2**A, multi-function electronic device **201***a* is shown in a block diagram view. Multi-function electronic device **201***a* comprises a processor **205** and a memory unit **207**, the processor **205** operatively coupled to the components of multi-function electronic device **201***a*. The memory **207** comprises a plurality of accounts **209**, which may be credit card accounts, banking accounts, merchant accounts, online accounts, cryptocurrency accounts, and combinations thereof. A motion detection module **210** is coupled to the processor unit **205** and to a set of motion detection units, which comprise a rate detection assembly **225**, an optical sensor array **230**, and a set of accelerometers **235**. The magnetic field is generated via a planar coil **220**, which is controlled by the processor unit **205** via a coil interface **215**. The rate at which the magnetic field changes polarity to encode the user data depends on the rate of relative movement detected by the rate detector. The multi-function electronic device **201***a* further comprises a real-time clock **240**, a touch-sensor array **245**, and a display **250**, each operatively coupled to the processor unit **205**. A user input may be made via the touch sensor array **245**, which may comprise a touch screen panel, a keypad, or a combination thereof. The display **250** is able to display an alphanumeric sequence, as well as graphical icons (such as a logo for a bank, or other images). Further, an optional backup power source **255** is depicted.

In one embodiment, the processor unit **205** is connected to the planar coil **220** and the motion detection units, via the motion detection module **210**. The processor unit **205** is responsible for determining the appropriate rate with which to output data from the planar coil **220**, wherein output data is encoded using alternating polarity of a generated magnetic field. The rate of the alternating polarity of the magnetic field is generated in accordance with the detected movement speed with which the card is swiped through the reader, in order for the reader to receive the encoded data at the appropriate rate. Magnetic card readers, which are designed to read conventional cards, are constructed to read data at specified input rates that correspond with the data density present in conventional magnetic card strips. The magnetic data symbols generated by the planar coil **220** are produced to align with the rate at which data is being read by the magnetic card reader. Accordingly, it is irrelevant if the multi-function electronic device **201***a* of the present disclosure is being swiped quickly or slowly, the planar coil **220** is controlled by the processor unit **205** to produce data at a substantially optimized rate, where the rate of data production is dependent on the rate at which the multi-function electronic device **201***a* is detected to be passing across the magnetic reader head.

FIG. **2**B depicts a multi-function electronic device **201***b* according to an embodiment of the present disclosure. Device **201***b* comprises a processor **205** and a memory unit **207**, the processor **205** operatively coupled to the components of multi-function electronic device **201***b*. The memory **207** comprises a plurality of accounts **209**, which may be credit card accounts, banking accounts, merchant accounts, online accounts, cryptocurrency accounts, and combinations thereof. A motion detection module **210** is coupled to the processor unit **205** and to a set of motion detection units, which comprise a rate detection assembly **225**, an optical sensor array **230**, and a set of accelerometers **235**. Additionally, a galvanic sensor **275** is coupled to processor unit **205**. The magnetic field is generated via a planar coil **220**, which is controlled by the processor unit **205** via a coil interface **215**. The rate at which the magnetic field changes polarity to encode the user data depends on the rate of relative movement detected by the rate detector. The multi-function electronic device **201***b* further comprises a real-time clock **240**, a touch-sensor array **245**, and a display **250**, each operatively coupled to the processor unit **205**. A user input may be made via the touch sensor array **245**, which may comprise a touch screen panel, a keypad, or a combination thereof. The display **250** is able to display an alphanumeric sequence, as well as graphical icons (such as a logo for a bank, or other images). Further, an optional backup power source **255** is depicted. Multi-function electronic device **201***b* further comprises a near-field communication (NFC) unit **260**, as well as a radio frequency identification (RFID) unit **265**, both of which are operatively coupled to the processor unit **205**. In one embodiment the NFC and RFID may share the planar coil for use as a radio frequency antenna, through the coil interface **215**. In one embodiment one or both the NFC and the RFID may have antennae dedicated to that individual sub-system. A universal serial bus (USB) connector **270** is coupled to the processor unit **205**. The functionality of the components with regard to exemplary uses of multi-function electronic devices **201***a* and **201***b* is described in greater detail in the following description.

A further aspect of the present disclosure provides a single multi-function electronic device that can be used for multiple banks or financial institutions. For example, instead of carrying a separate payment card for each account of a variety of payment card companies, a customer need only to carry a single device according to embodiments of the present disclosure. The capability of the multi-function electronic device to generate a multitude of payment numbers provides the ability of the multi-function electronic device to be associated with multiple accounts. Furthermore, inputs at the touch sensor array on the multi-function electronic device can be used to select the appropriate bank or credit provider account stored in the memory unit of the multi-function electronic device.

FIG. **2**C depicts a process of selecting an account from a plurality of stored accounts in order to perform a transaction with the selected account, according to an embodiment of the present disclosure. The process **280** begins at step **282**, where a plurality of accounts stored by the multi-function electronic device memory is displayed. The plurality of accounts **209** are stored by memory **207**, and are displayed using display **250**. A user indicates an account selected from the plurality of accounts at step **284**. The selection is able to be made by keypad or touch sensor array **245**, and an indication of the selected account can be displayed via display **250**. At step **286** the multi-function electronic device is configured according to account information associated with the selected account, which may include an account number, an expiration date, and other user information associated with the account (e.g. a username, PIN, password, email address, etc.). At step **288** the planar coil of the multi-function electronic device is encoded with a limited-duration payment number that is associated with the selected account. The limited-duration payment number is able to be generated according to the selected account, a timestamp, a transaction amount, an indicated merchant, user key or secrets, on-card unique hardware secrets, payment authority key or secrets, user input from the card interface, and other information associated with the transaction.

Movement Rate Feedback

The relative movement rate of multi-function electronic device **201***a* is detected by one or more of the set of motion detection units, comprising the rate detection assembly **225**, the optical sensor array **230**, and the set of accelerometers **235**. Each of the motion detection units detects the motion of the device **201***a* in a distinct manner. The rate detection assembly **225**, which is positioned alongside (but independent of) the planar coil **220**, is able to detect the location of a magnetic head reader as the rate detection assembly **220** is being passed through the card reader. The reader module of a conventional card reader comprises a metal head having a small gap at the tip of the head. A pickup armature resides in this gap, such that as the metal head passes over a card strip, an electric field is induced in the head reader pickup circuit. In one embodiment the rate detection assembly **225** is constructed of an array of auxiliary inductor coils and magnetic pickup coils. As the metal head of the card reader assembly passes over the arrangement of auxiliary inductor coils and magnetic pickup coils of the rate detection assembly **225**, a disturbance in the magnetic field flowing between the two is induced, generating a change in current and producing a detected movement signal. The change in current is detected by the motion detection module **210**, and is used to determine the rate of motion of the card reader head passing across the surface of the multi-function electronic device **201***a* (and therefore along the planar coil **220**).

The optical sensor array **230** is also operable to detect a movement rate of the multi-function electronic device **201***a* with respect to a conventional magnetic card reader. The optical sensor array **230** is disposed nearby the planar coil **220**, in order to accurately detect a movement rate in the region of the planar coil **220**. In an embodiment, the optical sensor array **230** is a thin strip parallel to, and extending along, the length of the planar coil **220**. The optical sensor array **230** determines a location of a minimum of received light, which corresponds to the region of a surface in nearest proximity to the optical sensor array **230**. The magnetic reader head of a conventional magnetic card reader extends furthest from the surface of the card reader, and therefore the detected minimum in received light at the optical sensor array **230** corresponds with the location of the reader head. By tracking over time the position of this minimum received light along the optical sensor array, a detected movement rate may be found.

The set of accelerometers **235** are also operable to detect a movement rate of the multi-function electronic device **201***a*. The set of accelerometers **235** are positioned in the multi-function electronic device **201***a* in order to effectively measure the position and acceleration of the multi-function electronic device **201***a*. In an embodiment, the set of accelerometers comprises groups of accelerometers, each group having one or more accelerometers disposed at orthogonal planes to each other, and each group capable of generating signals that allow for determination of the orientation, motion and acceleration of the multi-function electronic device **201***a*.

The detected movement signal is received by the motion detection module **210**. The detected movement signal is generated by any one of the set of motion detection units, or any combination of motion detection units of the set. For example, the movement detection signal is able to be generated by the combination of the rate detection assembly **225** and the optical sensor array **230**. In an embodiment, the movement detection module **210** is able to determine the movement rate of the multi-function electronic device **201***a* from the detected movement signals, and transmits the determined movement rate, and orientation to the processor unit **205**. In an embodiment, the motion detection module **210** sends the detected movement signal to the processor unit **205**, and the processor unit **205** determines the relative movement rate.

In one embodiment, the generation of the magnetic field by the planar coil **220** at a specified rate of alternating polarity is accomplished according to the following description. One or more of the motion detection units in the set of motion detection units (rate detection assembly **225**, optical sensor array **230**, and set of accelerometers **235**) detect a movement rate of the multi-function electronic device **201***a* with respect to a magnetic card reader, and signal the motion detection module **210**. The movement rate is provided to the processor unit **205**, which determines the appropriate rate for alternating the polarity of the magnetic field generated by the planar coil **220**. The processor unit **205** outputs instructions or data to the coil interface **215** at the determined rate, which in an embodiment is a digital-to-analog converter (a DAC) and acts to translate the signal from digital to analog in order to drive the planar coil **220** and produce the magnetic field. The instructions from the processor unit **205** are comprise binary code, which are output through a shift register to the coil interface **215**. The shift register outputs data at a rate proportional to the determined movement rate of the multi-function electronic device **201***a*—thus, a higher determined multi-function electronic device **201***a* movement rate has a corresponding higher output rate at the shift register, leading to a higher rate of alternating polarity at the generated magnetic field (i.e., encoded data symbols output more quickly). Conversely, a lower movement rate of multi-function electronic device **201***a* leads the processor unit **205** to control the shift register to output data at a lower rate, and consequently the rate of alternating polarity in the generated magnetic field is lower.

FIG. **3** illustrates an exemplary process **300** for determining the rate to alternate the polarity of the generated magnetic field of the multi-function electronic device, according to an embodiment of the present disclosure. At step **301** the process determines if a standard magnetic card reader is detected to be in proximity with the multi-function electronic device. If NO, the step repeats. If YES, the process

moves to step **303**. At step **303** a detection of a movement rate at which the body of the multi-function electronic device is moving relative to the standard magnetic card reader is made. The process continues at step **305**, wherein a magnetic field is generated by an inductor assembly comprised by the multi-function electronic device, the magnetic field having a target rate of alternating polarity that is based on the detected movement rate from step **303**. The process then repeats at step **301**, determining if a standard magnetic card reader is (or remains) in proximity to the multi-function electronic device. In this manner, while a standard magnetic card reader is detected to be in proximity to the multi-function electronic device, the movement rate of the multi-function electronic device is determined and the polarity and orientation of the generated magnetic field is alternated at the appropriate rate, to recreate the data as described above, at the correct rate, in order to clock out the data to be conveyed to the magnetic strip reader, at a rate matching the action of an ordinary magnetic strip card through same the magnetic card reader.

Security

Security is an area of concern for payment card holders, as the small form factor makes theft quite easy, and additionally there are many ways for a malicious third-party to record the account number of a payment card in order to later make fraudulent transactions on the account. Embodiments of the present disclosure address security concerns of a payment card owner on several fronts.

In one aspect, security of the multi-function electronic device is enhanced by providing a means of locking the multi-function electronic device in order to prevent use, until such time that a valid user input is entered. Embodiments of the present disclosure provide a multi-function electronic device having a region for receiving human input, e.g., touch sensors which are able to be formed by contacts that a user can press (e.g., the touch sensor array **245** of FIGS. **2**A-**2**B). FIGS. **4**A-**4**B illustrate a user interacting with a multi-function electronic device **401** via a keypad or touch sensor array **445**. In FIG. **4**A, the multi-function electronic device **401** is in a locked state. A display **450** is able to display a message to the user, for instance, the message "device locked" or "enter password," or question prompts which guide the user to respond with answers through the key-pad or the touch sensor, to certain preset questions, that confirm personal knowledge known only to the associated user. The touch sensor array **445** enables user interaction with the multi-function electronic device **401**. An exemplary use of the touch sensor array **445** is an input of a currency amount to be used in a transaction. The touch sensor array **445** is able to include buttons, or a touch-sensitive pad, or a combination of the two. Other embodiments of the touch sensor array **445** allowing a user to input data to the multi-function electronic device **401** are consistent with the spirit and scope of the present disclosure.

In order to unlock the multi-function electronic device **401** and enable a transaction or other usage, the user inputs data via the touch sensor array **445**. FIG. **4**B illustrates the user inputting a password via a gesture **470**, which operates to unlock the multi-function electronic device **401**. The display **450***b* is able to display a message indicating the multi-function electronic device **401** is unlocked and ready for use, for instance, display **450***b* may display the message "unlocked," or it may display an account number associated with the multi-function electronic device **401**.

Embodiments of the present disclosure provide additional functionality for the touch sensor array **445**. For example, there may be touch contact terminals that a user can press to wake up the multi-function electronic device **401**, to cause the battery to supply power, or to place the multi-function electronic device **401** in a power reduction mode when it is not being used. In an embodiment, if any number other than the correct password is entered multiple times, or if there is an attempted usage of the multi-function electronic device **401** without entering in a password, an automatic phone call may be triggered to the appropriate fraud protection authorities.

In one embodiment of the present disclosure, the display **450** is a thin-film liquid crystal display ("LCD"). The display **450** is able to have multiple uses. In one embodiment, the display **450** can be used to cue the user for a security question upon input of an improper password. Or if fraud protection services need to contact a customer, they can verify the customer's identity by transmitting a security question to the display **450** of user's multi-function electronic device **401**, to which the user would need to respond correctly using the input buttons of touch sensor **445** on the card.

Limited-Duration Payment Number

A further security feature of the multi-function electronic device provided in the present disclosure is the capability of producing a limited-duration payment number for performing transactions using accounts of the card. The multi-function electronic device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction. The power source is able to activate the processor unit such that a unique number may be generated by the multi-function electronic device and verified by the payment authority according to the timestamp and the transmitted user information. The limited-duration payment number is able to be produced at the time the multi-function electronic device is performing a transaction, and is able to be generated according to the user's private information, a bank information, information regarding the facility performing the transaction, and the time of day. The limited-duration payment number is able to be limited to only one transaction, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid. As detailed above, if an expired limited-duration payment number is attempted to be used for a transaction, the transaction is denied and an automatic notification is able to be made to a payment authority in order to notify the user and to prevent transactions on the account. The transaction count is able to be determined through the action of passing the card through magnetic reader, and the process of transmitting the payment number to the card reader.

In one embodiment, the number on the front of the card is able to be a full or partial number. In an embodiment, the number displayed on the multi-function electronic device is a static number, but the number transmitted during a transaction is a limited-duration payment number as described above. The number displayed on the multi-function electronic device may not necessarily be a static number. For example, the first four and last four digits of the payment number are able to be fixed, while the remaining eight digits can be dynamically generated. As the device is read by the machine, part or all of the number may be dynamically produced at the time the device is read. As described above, the dynamic part of the limited-duration payment number generated may be based on the user's private information, the user's bank information, the time of day or the facility

that is reading the card. Further, the expiration date of the multi-function electronic device can also be dynamically generated.

Effectively, embodiments of the present disclosure provide a multi-function electronic device that has no fixed number, as illustrated in FIG. **11**, and therefore the account cannot be compromised. Only the number generated at the instant of the multi-function electronic device transaction matters. Accordingly, unauthorized use of the multi-function electronic device is highly unlikely, because a transaction cannot be conducted with an expired limited-duration payment number, or only the static portion of the payment number. In one embodiment of the present disclosure, sufficient dynamically generated numbers are provided for on the multi-function electronic device such that a unique payment number can be generated for each transaction. In this embodiment, the multi-function electronic device of the present disclosure effectively acts as a unique per-transaction payment device.

With reference to FIG. **2**A, **2**B, in one embodiment, the process steps enabling a card transaction are as follows. A multi-function electronic device (e.g., multi-function electronic device **201***b*) is connected to a computer system (e.g. computer system **590**, FIG. **5**), via any of the connection means available to the multi-function electronic device (USB **270**, NFC **260**, and RFID **265**). User data and other essential information, such as account information, are downloaded to the multi-function electronic device. For example, for an account designed for online transactions, user account information will likely include an account email and an account password. The account may be for example a bank account, a credit account, a merchant account, an online transaction account, or a cryptocurrency. In one embodiment a currency amount is also downloaded, which is made accessible to the multi-function electronic device **201***b* for transactions. In an alternative embodiment, rather than a currency amount being downloaded to the multi-function electronic device **201***b*, the user account information (e.g., username and password) is stored such that a subsequent authorized multi-function electronic device **201***b* transaction is automatically pre-authorized to deduct (or credit) the entered transaction amount at a stored account. In an embodiment, a user uses the touch sensor array **245** of the multi-function electronic device **201***b* in order to input the user information, including the amount of currency to be stored. The information entered by the user is able to include an account source of a transaction (e.g., bank account, credit account, merchant account, ATM, online payment service, or a cryptocurrency), as well as a type of transaction to be made (e.g., as a debit card, as a credit card, or as a user account). In another embodiment, the information is entered using the computing system to which the multi-function electronic device **201***b* is connected.

Transactions may be authenticated on the specified account by entry of the username and password for the account during the transaction, using the touch sensor array **245**. In an embodiment, a password for an account is represented by a user input (such as a gesture, a swipe, and/or an unlock keycode) which is entered on multi-function electronic device **201***b* during a transaction for account authentication. According to an embodiment of the present disclosure, a user that has "primed" the multi-function electronic device **201***b* for a transaction has already performed a security authentication on the card, and therefore a subsequent card transaction is able to be pre-authorized to perform the transaction without further user authentication steps. The priming action can be a tap of the multi-function electronic device **201***b* detected by accelerometers **235**, or a gesture, swipe, or a key input received by touch sensor array **245**.

A transaction is able to be communicated using the planar coil **220**. In one embodiment, when the transaction is a payment transaction, a limited-duration payment number is generated. A user inputs an amount for the transaction using the touch sensor array **245**, and the limited-duration payment number is generated to correspond with the entered amount. The binary data corresponding to this limited-duration payment number is sent from the processor unit **205** to the coil interface **215**, where it is converted to an analog signal in order to drive the planar coil **220** to generate a magnetic field having an alternating polarity corresponding to the encoded data of the limited-duration payment number.

Online Transactions

FIG. **5** displays the multi-function electronic device **501** in connection with a computing device **590**. In one embodiment, the multi-function electronic device **501** is able to be used to make online purchases. In one embodiment, the multi-function electronic device **501** is equipped with a means **570** for communicating with the USB port on a computer or other device in order to make online purchases. In one embodiment the multi-function electronic device **501** may have an area cut out, such that contact terminals corresponding to a USB cable connector are contained within, enabling connection of a USB cable (e.g., a micro-USB connection). When performing online transactions, the multi-function electronic device **501** can uniquely generate a limited-duration payment number (as described above) for online purchases. The multi-function electronic device **501** receives a user input indicating that a transaction is imminent, and an authorization. The user input is able to comprise a gesture, a swipe, a key input sequence, and combinations thereof. The limited-duration payment number is able to be displayed on the front display of the multi-function electronic device **501**. In one embodiment, the multi-function electronic device **501** is able to use RFID **265** or near field communication NFC **260** technology in order to connect to a personal computer **590**. This enables a per-transaction, limited-use payment number, enhancing the security of the payment account by substantially negating the possibility of a theft of the payment number used to perform the transaction leading to account compromise. See also, for example, FIG. **10**.

According to an embodiment, the transaction is able to include information regarding a user account, such as an email address of the user, and upon reconnection of multi-function electronic device **201***b* to a computer system (for instance, computer system **590**), the transaction information stored on multi-function electronic device **201***b* could be "replayed" by the computer system in order to finalize the transaction.

In one embodiment, a means of limiting an available credit amount are provided. According to the download process described above, the multi-function electronic device is able to have a total credit available. The multi-function electronic device is able to reference the total credit available in subsequent transactions, and will provide limited-duration payment numbers corresponding to amounts up to, but not exceeding, the remaining credit available to the multi-function electronic device. An attempt to perform a transaction having an amount exceeding the remaining credit available will not result in a valid limited-duration payment number, and therefore an authenticated transaction cannot proceed. In general, the multi-function electronic device will only successfully generate a limited-duration

payment number if the proper conditions for a transaction are determined to be present. The proper conditions for a transaction comprise a correct identification having been made by the user (via a gesture, swipe, and/or key input) and an amount for the transaction indicated to be less than the total credit available to the account indicated for the transaction.

Device-to-Device Transactions

In addition to transactions performed using conventional magnetic card readers (such as at point-of-sale locations, banks, and automated teller machines (ATMs)) and via cable connection with a computing device, transactions performed wirelessly between a device and a device (e.g., card-to-card, card-to-computer device having a reader dongle, card-to-ATM) are provided according to embodiments of the present disclosure. See, for example, FIGS. **8** and **10**. For simplicity, the following describes a device-to-device transaction, but it will be understood that card-to-device transactions are similarly provided.

FIG. **6** illustrates a device-to-device transaction according to one embodiment. A first multi-function electronic device **601***a* comprises a display **650***a*, and is in contact with a second multi-function electronic device **601***b*. A contact interaction between the devices is indicated by interaction **680**. In one embodiment, the contact interaction is a tapping of a device **601***a* against another device **601***b*. In another embodiment, an optical sensor array at one or both of the devices detects interaction **680**. In another embodiment, interaction **680** indicates a swipe of a device **601***a* across another device **601***b*. In one embodiment a user input through the key-pad initiates and enables a transaction from first device to second device. In one embodiment the presence of second device in preparation for device-to-device transaction is confirmed through "polling", the process of which involves transmission of data between devices, and confirmed receipt of transmitted data by response received from second device received at first device, including information confirming receipt of the information, by second device.

The planar coil comprised by each of multi-function electronic device **601***a* and multi-function electronic device **601***b* is able to be a means of transferring information for a transaction, e.g., such as an antenna. Once either, or both, of multi-function electronic device **601***a* and multi-function electronic device **601***b* detect interaction **680**, a transaction is able to be completed via generation of a magnetic field at one card and reception of the magnetic field (i.e., reading) at the other card. In this manner, the device (e.g., multi-function electronic device **601***a*) receiving the transaction information operates its planar coil in an antenna mode. This enables multi-function electronic device **601***a* and multi-function electronic device **601***b* to authentically perform a transaction, and to transfer a currency between multi-function electronic device **601***a* and multi-function electronic device **601***b*. As described above, in an embodiment the transaction is able to use a limited-duration payment number to encode the transaction.

In an embodiment, a set of accelerometers is used to detect the beginning of the transaction, for instance, a transaction performed by a swipe of multi-function electronic device **601***a* across multi-function electronic device **601***b*. Further, the set of accelerometers can detect a "priming" action for a multi-function electronic device, i.e., an indication for a multi-function electronic device that a transaction is imminent. The priming action can be a tap of the multi-function electronic device **601***a*, or tapping the multi-function electronic device **601***a* against the multi-function electronic device **601***b*. In one embodiment, a touch sensor array is able to be used for the priming action.

In an embodiment of a device-to-device transaction, one device (e.g. **601***a*, the device of the user having a currency debit) generates the limited-duration payment number, which is transmitted via the device's planar coil. The multi-function electronic device of the recipient (e.g., **601***b*, the card of the user receiving a currency credit) receives the encoded data via the planar coil, acting as an antenna, and the coil interface is able to convert the received signal into a digital signal understood by the processor to be the limited-duration payment number, identifying both the correct account and the amount of the transaction.

In one embodiment, the multi-function electronic device **201***b* stores cryptocurrency information in processor unit **205**. The cryptocurrency information stored is able to include a plurality of cryptocurrency addresses, a plurality of private keys, and a plurality of public keys. The multi-function electronic device **201***b* is able to perform a transaction, as described above, using a cryptocurrency as the specified account. In one embodiment, the multi-function electronic device **201***b* is able to hash a portion of the transaction, using the processor unit **205** and the real-time clock **240** along with user information pertinent to the cryptocurrency account and the transaction. A subsequent connection of the device **201***b* to a computing device provides a means of connecting to the cryptocurrency servers and finalizing the transaction. Further, the multi-function electronic device **201***b* is able to sign a cryptocurrency transaction by, for instance, receiving a prompt at the display **250** to input a dynamic PIN specific to the transaction, which is able to be entered by touch sensor array **245**.

In a device-to-device cryptocurrency exchange, a record of the transaction can be made according to the following. A first device (e.g. **601***a*) making a deduction with an amount indicated via touch sensor array **245** is able to generate a record of the transaction and store the record in the device memory, while a second device (e.g. **601***b*) receiving the cryptocurrency is able to generate a confirmation of the received transaction amount. In one embodiment, the amount indicated is provided by the receiving device **601***b*. The hashed record of the transaction contains the unique information of each user, along with the transaction amount. The success or failure of the transaction is able to be displayed on the respective displays of devices **601***a* and **601***b*.

Account Theft and Unintended Use Prevention

A security concern for conventional credit cards utilizing wireless communication means is the ability of a thief to access and/or copy user information through un-detected interaction with the wireless communication means. Sensitive and confidential information can be gleaned via, for example, "listening-in" on an RFID interaction between a credit card and a contactless reader, recording the characteristics of the interaction, and replicating certain characteristics to fake an authorized transaction. While to a great extent security concerns are addressed by the usage of limited-duration payment numbers and other security features provided for by the device of the present disclosure and previously described, a further security feature regarding the wireless communication means of the multi-function electronic device is described herein.

In one embodiment, wireless communication means of the multi-function electronic device **201***b* are in a powered-down, or disabled, state prior to receiving an authenticated activation signal from a user. Upon receiving the activation signal, the communication means (e.g., NFC **260**, RFID **265**,

and planar coil **220**) are activated, enabling the multi-function electronic device **201***b* to conduct a transaction. The activation signal can originate from one (or a combination) of the set of motion detection units (rate detection **225**, optical sensor array **230**, and accelerometers **235**), the touch sensor array **245**, and the galvanic sensor **275**. The galvanic sensor **275** is operable to detect a contact of human skin, via a current produced at the sensor **275** upon such contact. See also, for example, FIG. **8**. In an embodiment the galvanic sensor **275** is comprised of metallic contacts disposed on opposite sides of, and isolated by, the body of multi-function electronic device **201***b*. In one embodiment, the current produced by user contact with the galvanic sensor **275** contacts is sufficient to provide small amounts of energy in order to power components of the card. For example, energy produced is able to power the processor unit **205** and the RFID **265**. In one embodiment the galvanic sensor **275** further comprises two conducting surfaces separated by a junction, and the galvanic sensor **275** is configured as a thermoelectric generator (e.g., via the Peltier effect, the Seebeck effect, or a combination). For example, heat applied at one surface of the multi-function electronic device **201***b* may lead to differential heating between the opposing, separated conducting surfaces of the galvanic sensor **275**, generating an electric current and powering a subset of, or all of, the components of multi-function electronic device **201***b* (e.g., the processor unit **205**, the NFC **260**, and the RFID **265**).

In an embodiment, the communication means are activated only so long as the activation signal continues to be detected. In another embodiment, the communication means are activated for a specified amount of time following detection of the activation signal. For example, if using the multi-function electronic device **201***b* in an ATM (or other device) preventing continuous human contact, the activation signal is able to be a swipe, gesture, or key input sequence entered via the touch sensor array **245**, which activates the device for a specified duration (for instance, one minute). In an embodiment the detection of motion through accelerometer input indicates activation by a valid user. In one embodiment the specific motion detected through accelerometer input corresponding with a specific user action, such as a "flick", "swipe", "spin", "wave", "tap," may be used to initiate activation, wherein the motion is not normally generated at idle and during periods of inactivity. For example the motion not being generated accidentally while the device is stored in a user's wallet, carried while the user is actively moving, or is being handed from user to a clerk at a point of transaction. In one embodiment the specific motion, or sequence of motions, may be associated with a user, and stored on the device memory, such that performing the correct sequence when prompted can confirm the possession of the device by the known owner, thus initiating activation and enabling usage.

FIG. **7** depicts a process of selectively enabling the communication capability of the multi-function electronic device according to an embodiment of the present disclosure. The process **700** begins at step **701**, where an input signal is received at the multi-function electronic device from a user. The input signal is able to be generated by any one, or combination, of a plurality of input means, where the input means comprise: a swipe gesture received at a touch sensor array; a key press sequence; an accelerometer sensor indication of multi-function electronic device motion; and a galvanic sensor indication that the device is in a user grasp. The input received from the user enables operation of a near-field communication (NFC) unit of the multi-function electronic device. In one embodiment, the NFC unit is disabled prior to receiving the input signal. In one embodiment, an RFID communication unit is disabled prior to receiving the input signal, and is activated by the input signal. In one embodiment, the planar coil is disabled prior to receiving the input signal, and is activated by the input signal.

The multi-function electronic device, following enablement of the NFC unit, receives an indication of an amount of currency for a transaction at step **703**. At step **705**, the multi-function electronic device generates a limited-duration payment number, which at step **707** is transmitted to a recipient of the transaction. In one embodiment, the limited-duration payment number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.

In the foregoing description of process **700**, the ordering of the process steps is exemplary and should not be construed as limiting. Alternative ordering of the process steps is consistent with the present disclosure, as conceived by one skilled in the relevant art.

In one embodiment of the present invention, a credit card comprises a dynamic magnetic strip incorporating a main inductor assembly from which magnetic field data symbols are dynamically generated. In one embodiment the inductor assembly may be a planar coil formed within the plastic that the credit card is composed with. The advantage of using a planar coil is that it can produce the same magnetic field interaction that a traditional magnetic strip on a conventional credit card can produce when it is passed through a reader. Similar to a traditional plastic credit card, the planar coil can also produce a magnetic field that can be read by a pickup (or "transducer"). The pickup produces electric current in the coil that, in turn, produces a magnetic field that is read by the pickup. Accordingly, the planar coil can be read in the same way as the magnetic strip on a traditional plastic credit card. The magnetic field produced by the planar coil would behave identically to a traditional magnetic strip.

In one embodiment, alongside the main planar coil, auxiliary rate detection assembly independent of the main inductor assembly would be provided to assist with the alignment of the production of data from the loop as it is being passed over the head of the credit card reader. The reader module of a traditional credit card reader comprises a metal head with a small gap on the tip of the head. This gap is where the pickup armature resides, so that when the metal head passes over the credit card strip, an electric field is induced in the head reader pickup circuit. In one embodiment the auxiliary rate detection assembly is constructed of an array of auxiliary inductor coils and magnetic pickup coils, alongside the main coil. As the metal head of the card reader assembly passes over the arrangement of auxiliary coils and pickup circuits, a disturbance in the magnetic field flowing between the two generates a electrical current change that is detected by a rate detection circuit so as to detect the rate of motion of the card reader head passing across the surface of the card and therefore along the main induction assembly. The purpose of this is to allow the determination of the rate or production of magnetic data symbols in the main inductor assembly to align with the rate at which data is being read by the reader, according to the data density of standard card magnetic strips. Accordingly, it is irrelevant if the credit card of the present invention is being swiped fast or slow, the main inductor assembly produces data at just the right rate depending on the rate at which the card is detected it is being passed over the reader's head.

In one embodiment, a microprocessor is connected to the main coil and the alignment pickups. The microprocessor is responsible for producing the data from the coil at the appropriate rate in accordance with the speed with which the card is swiped through the reader. As shown in FIG. **1**, the auxiliary coil detects the rate at which the credit card is being swiped. The microprocessor then uses this information to produce the data from the main planar coil at the appropriate rate for the credit card reader.

In addition, the credit card of the present invention comprises a real time clock that can produce a cryptographically worthy timestamp for each interaction and a battery back up that can be used to power up the microprocessor. Further, the card can comprise additional human inputs, e.g., touch sensors which can be formed by contacts that a user can press. For example, there can be contacts that a user can press to wake up the card, to cause the battery to supply power, or to put the card to sleep when it is not being used. There can also be additional inputs to key in customer specific information. For example, there can be inputs to key in a password or any other kind of unique identifier. If any other number besides the password is entered multiple times, or if there is attempted usage of the card without entering in a password, an automatic phone call may be triggered to the appropriate fraud protection authorities.

In one embodiment, the number on the front of the card can be a full or partial number. The number may not have to necessarily be a static number. For example, the first four and last four digits of the card number can be fixed while the remaining eight can be dynamically generated. As the credit card is read by the machine, part or all of the number may be dynamically produced at the time the card is read. The dynamic part of the number generated may be based on the user's private information, the user's bank information, the time of day or the facility that is reading the card. Further, the expiration date of the card can also be dynamically generated. Effectively, a credit card can be created that has no fixed number and therefore cannot be stolen. Only the number generated at the instant the card is being used matters. Accordingly, unauthorized use of the card is nearly impossible because no transaction can be conducted with only the partial static part of the payment number. In one embodiment of the present invention, enough dynamically generated numbers are provided for on the credit card such that a unique payment number can be generated for each transaction. In this embodiment, the credit card of the present invention effectively acts as a unique per transaction credit card.

In embodiments of the present invention comprising dynamically created payment numbers, a single credit card can be used for multiple banks. For example, instead of carrying a separate credit card for all the different credit card companies, a customer would only need to carry a single card and one of the inputs on the front of the card can be used to select the appropriate bank or credit provider.

In one embodiment of the present invention, a thin film liquid crystal display ("LCD") can be fitted on the card so the credit card can have a display screen. The display can have multiple uses. In one embodiment, the display can be used to ask the user a security question if an improper password is entered. Or if the fraud protection services need to contact a customer, they can verify the customer's identity by transmitting a security question to the user's credit card screen to which the user would then need to respond correctly using the input buttons on the card.

In one embodiment, the credit card of the present invention could also be used to make online purchases. In this embodiment, the card could use RFID or near field technology so that it can connect to a personal computer and be used to uniquely generate a payment number for online purchases. The number could also, in one embodiment, be displayed on the front LCD of the card. In one embodiment, the card may also be equipped with a means for communicating with the USB port on the computer in connection with making the online purchases.

TABLE 1

1. An apparatus for conducting credit transactions comprising:
a device with the similar dimensions and thickness to a standard credit card
an inductor assembly integrated into said device capable of generating a programmed magnetic field at a location on the device where it will come into proximity to a standard credit card magnetic-strip reader
the inductor assembly being operable to be read by a magnetic pickup of an electronic credit card reader;
at least one auxiliary rate detection units adjacent to said inductor assembly, wherein said at least one auxiliary detection unit is operable to detect a rate at which said device, including said inductor assembly, is passed through said electronic credit card reader; and
a microprocessor operatively coupled to said inductor assembly and said at least one detection unit, wherein said microprocessor is operable to simulate magnetic-strip data fields using the inductor assembly, at a rate determined from said auxiliary detection units.
2. A method of Claim 1, wherein the inductor assembly is a planar coil which is a looped inductor with dimension roughly equal to, and along the axis of, the standard credit-card magnetic strip
3. A method of Claim 1, wherein said detection assembly consists of a plurality of motion rate detection units, which may comprise inductor coils and companion magnetic-field pickup coils, each of which is able to detect the proximity of metallic objects, such as magnetic-strip reader heads, passing through the magnetic field created by said inductor and detected by said pickup coil.
4. A method of Claim 1, wherein said device may incorporate a plurality of touch sensors arranged along the surface of said device which may;
allow user input of information,
allow introducing a transaction specific identifier,
to confirm/deny transaction information,
to operate in sequence, or with a gesture across said sensor for the purpose lock/unlock or control access for transactions
5. A method of Claim 4, wherein said device contains a real-time clock or counter unit which generates a sequential parameter when the card is read by said credit

TABLE 1-continued

card reader, and which along with certain user information, transaction identifiers, user secrets, payment authority secrets is combined to generate a limited-use payment number, which has a limited recurrence, is limited in scope of use to a predetermined number of authorized transactions
6. A method of Claim 5, wherein the time, sequence, user, payment authority and other information is similarly combined by credit card processing facility to generate a payment number for comparison to the number transmitted by the credit card reader, for the purposes of authenticating said number is from a recognized card used in a user-authorized transaction
7. A method of Claim 1, wherein said device incorporates a display allowing payment number, time, passcodes, sequence codes, amounts and other credit card transaction information to be displayed for user, merchant, bank or credit card authority
8. An Apparatus for conducting credit transactions comprising, wherein the edge of said device contains a connector for connection to standard computing devices such as a USB interface.

The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as may be suited to the particular use contemplated.

Embodiments according to the invention are thus described. While the present disclosure has been described in particular embodiments, it should be appreciated that the invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

What is claimed is:

1. A method of performing a payment transaction, the method comprising:

receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and,

wherein the authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a gesture sensor, a motion sensor, and a biometric sensor; and,

receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and,

displaying, on a display of the device, a transaction payment request and at least a portion of an original static issuer-supplied payment account information associated with a payment method, for a user selection in paying the payment request; and,

retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and,

dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and,

using said limited-use payment information in place of at least a portion of said selected original issuer-supplied payment information for the transaction; and,

combining of said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information; and,

transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and,

receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the transmitted complete device payment information by a payment processor authority and a payment issuer authority; and,

visually conveying the transaction payment authorization status via a user-interface displayed on said display.

2. The method of claim **1**, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.

3. The method of claim **1**, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.

4. The method of claim **3**, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and,

wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.

5. The method of claim **3**, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and,

wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and,

wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and,

a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction

sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and,

an adjusting of said transaction sequence counter count on a per transaction basis; and,

an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.

6. The method of claim **3**, wherein the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and,

a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and,

a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid; and,

a conveying of said validation result as a declining or accepting of said transaction payment; and,

upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.

7. The method of claim **3**, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including:

a confirmation result of payment authority authenticating said device-transmitted limited-use payment information,

a confirmation result of payment authority authenticating said device-transmitted complete device payment information,

an NFC transaction status,

a transaction payment amount,

a payment facility wherein the transaction was performed,

a merchant information,

an original issuer payment account information,

an original payment issuer information,

a request for an authorized-user approval of the transaction,

a payment processing status,

an issuer payment approval status, and

a payment completion status.

8. The method of claim **1**, wherein the generating the limited-use payment information is comprising:

a device-specific account number; and,

a device-internal transaction sequence counter count; and,

an information unique to the user and device which does not pass in the transaction; and,

at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and

wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.

9. The method of claim **8**, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.

10. The method of claim **9**, wherein the generating the limited-use payment information further utilizes a secure combination with a device key, and a payment issuer secret.

11. The method of claim **1**, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of:

a device payment transaction sequence counter count, and

at least one of a set comprising:

a device-specific internal information associated with said device and also known to a payment processing authority; and,

at least one payment processing authority-specific information provided by a payment processing authority; and,

a payment issuer specific information provided by a payment issuer.

12. The method of claim **1**, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.

13. The method of claim **1**, wherein the generating the limited-use payment information utilizes a merchant identifying information.

14. The method of claim **1**, wherein the generating the limited-use payment information utilizes a transaction facility information.

15. The method of claim **1**, wherein the generating the limited-use payment information utilizes a payment amount.

16. The method of claim **1**, wherein the generating the limited-use payment information utilizes a payment facility type.

17. The method of claim **1**, wherein the generating the limited-use payment information utilizes an online transaction information.

18. The method of claim **1**, further comprising:

dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and

wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram; and,

wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.

19. A method of performing an online payment transaction, the method comprising:

receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device;

a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and,

upon an authorizing of a valid device user, displaying at least one user-selectable payment account option, and requesting a user approval of payment, via the touch-screen display user-interface;

receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;

generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and

combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and,

wherein the receiving of a user payment approval authorization through the user-interface of the electronic device, is comprising a displaying on said display at least a portion of information comprising: the payment request, the merchant, the amount, and the transaction information; and,

receiving a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method; and,

on receiving said user payment approval authorization input, a transmitting by the wireless interface of the approved complete payment information for the online transaction.

20. The method of claim **19**, further comprising:

dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuing authority, and wherein dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count, a user information, a payment account number, information and secrets known to a payment processing authority; and

wherein further, said dynamically generating said card validation value number results in a one-time limited-use payment information, on incrementing the device transaction sequence counter count on each transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.

21. The method of claim **19**, wherein at least a portion of said limited-use number comprises a static device account number,

and wherein the static device account number is of a limited scope of valid use to a specific device,

and wherein further a payment processing authority provides said device account number unique for the specific electronic device, in place of payment issuer information, in performing payment transactions by the electronic device, and further comprising:

performing a payment transaction by the electronic device including the dynamically generated limited-use number;

combining the dynamically-generated number and the static device account number within a device-generated complete payment information; and

conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and

wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage.

22. The method of claim **19**, further comprising:

generating a limited-use security code number for use in place of a card issuer card security code, by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter; a device account number; a payment account information, device secrets; payment processing authority secrets; and

displaying the limited-use security code number on the user-interface of the device display.

23. The method of claim **19**, wherein a payment processing authority verifying and authorizing a transmitted limited-use number based on a time of use, and cryptographically combining a transaction sequence count information; a device account number; a user account information; a payment issuer information; a payment processing authority secrets; a transaction information; and,

further comprising: receiving an authorization of said transaction, responsive to verifying a valid limited-use number appearing in a transaction information in place of the payment issuer information; and

a rejecting by the payment processing authority, on a detecting as invalid at least one verification test, from a set of tests comprising:

a mis-matching of the transacted limited-use number, and the authority cryptographically-combined number;

a transactional use of a device account number outside of its limited scope of valid payment reader facility use;

a transactional use outside of a valid time window;

a transactional re-use of a number limited to a one-time use; and,

a transactional use of an expired number outside of a limited time-of-use.

24. The method of claim **19**, wherein the user selecting of a payment method at an electronic device comprises receiving a user touch input selection, via the user interface, of a displayed payment method option, on the device touch-screen display interface.

25. A non-transitory, computer-readable medium storing computer executable instructions that when executed by one or more processors, cause the one or more processors to:

accept a priming action of the electronic device by an identified valid device user, identified from the device inputs;

enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user;

display a summary of online purchase information including the merchant information and the purchase amount; and,

display at least one selectable issuer payment account methods on a display; and,

receive a payment selection and approval authorization from said valid device user via a human input sensing at the device; and

responsive to receiving a valid user transaction payment approval, generate a device-specific limited-use pay-

ment information for use in place of at least a portion of said selected issuer payment account information on the device,

form a complete combined device payment information from a dynamically generated portion and a statically generated portions stored in a memory of the device,

wherein the communication interface is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction; and

wherein further the processor is operable to receive an approval and a denial confirmation from an online payment facility of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction.

26. The non-transitory, computer-readable medium of claim **25**, wherein the executable instructions further cause the one or more processors to:

receive the priming action of a user via the device human input sensors;

identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of human to device input challenges comprising:

a correct passcode touch entry sequence,

a correct touch gesture,

a touch input of a known device user,

a biometric recognition of a valid user,

a biometric sensing of a valid user's skin touch,

a touch input sensor recognition of a unique customer identifier,

a security question which a valid user could answer correctly, and

receiving a correct user response input, from a security challenge presented on the device display; and

responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization.

27. The non-transitory, computer-readable medium of claim **25**, wherein the one or more processors include a cryptographic processor, and wherein the executable instructions further cause the one or more processors to:

cryptographically compute a dynamically generated one-time-use cryptogram number,

and combine said dynamically generated portion with a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method; and,

wherein further said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction; and,

wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority; and,

wherein further said static device-specific device account number is known to a payment issuer, and has a device-specific expiration date of limited duration of validity; and,

wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram,

and transmitting said complete device payment information when said issuer payment account method is selected.

28. The non-transitory, computer-readable medium of claim **25**, wherein the executable instructions further causes the one or more processors to perform:

a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device; and,

a generating of a limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers; and,

wherein the one or more device processors are further operable to combine said limited-use static device account information and said one-time use cryptogram number(s) to produce the complete combined device payment information; and,

wherein the one or more device processors are further operable to transmit said complete payment information in place of said user-selected payment account information in a device payment transaction; and,

wherein the one or more device processors are further operable to display at least a portion of said user-specific selected account information associated with said complete device payment information used during said transaction, via a user interface disposed of the device.

29. The non-transitory, computer-readable medium of claim **25**, wherein the executable instructions further cause the one or more processors to dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority, and selected from a set of information known and stored at both said payment authorities, and on said device, including:

a transaction sequence counter,

a device account number,

a device account expiration date,

a device secret,

a payment processing authority secret,

a user information,

a payment account information,

a payment issuer information,

a payment amount, transactional information; and,

wherein said one or more processors uses said one-time limited-use cryptogram number in place of at least a portion of an issuer's static payment information, in a payment transaction using said payment account; and,

wherein said payment authorities are operable to recognize from the transactional payment information, the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information; and,

wherein said payment processing authorities are operable to deny as invalid a transaction including a cryptogram not matching an authority computed cryptogram; and,

wherein said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,

wherein said device is operable to receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device.

30. The electronic device of claim **25**, further comprising a processor and a non-transitory, computer-readable medium storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to dynamically generate a one-time limited-use cryptogram number by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including:

a transaction sequence counter;

a user payment account number;

a device payment account number;

a device secret; device keys;

a payment issuer original account information;

a payment issuer device account information;

a payment processing authority secret;

a transaction information;

and a user private information; and,

wherein said cryptogram is operable to be used in place of at least a portion of an issuer's static payment information, in a payment transaction for said selected payment account; and,

wherein said payment processing authority is operable to deny as invalid, a transaction including a cryptogram not matching a payment processing authority computed cryptogram; and,

wherein said payment processing authority is operable to approve as valid, a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,

wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device; and,

wherein said user device is operable to emulate the behavior of an issuer account payment transaction, when said complete device payment information is used in electronic payment facilities.

* * * * *