(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 704 395 B1

(51) Int. Cl.: G06Q 20/16 (2012.01)
G06Q 20/32 (2012.01)

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT

(21) Anmeldenummer: 00146/11

(22) Anmeldedatum: 28.01.2011

(43) Anmeldung veröffentlicht: 31.07.2012

(24) Patent erteilt: 15.09.2015

(45) Patentschrift veröffentlicht: 15.09.2015

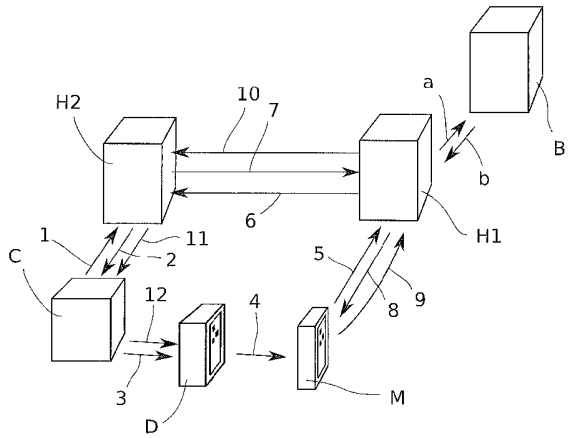
(73) Inhaber:
InVisible GmbH, Erlachstrasse 25
8003 Zürich (CH)
GnostX GmbH, Sempachstrasse 13
3014 Bern (CH)

(72) Erfinder:
Matthias Günter, 3014 Bern (CH)
Jens-Christian Fischer, 8055 Zürich (CH)
Simon Günter, 3014 Bern (CH)
Manuel Günter, 8037 Zürich (CH)

(74) Vertreter:
VENI GmbH, Villa de Meuron, Buristrasse 21
3006 Bern (CH)

(54) System und Verfahren zur gesicherten Übertragung von Werten.

(57) Die Erfindung betrifft ein System und Verfahren zum sicheren und zuverlässigen Durchführen von Transaktionen. Die Erfindung ermöglicht in einfacher Weise mittels Kennungen, verschlüsselten Verbindungen, der Verwendung von mobilen Geräten (M) mit Anschlusskennung und Kamera über grafische Darstellung der Kennung Transaktionen, auch insbesondere finanzieller Natur, durchzuführen.



Beschreibung

Technisches Gebiet der Erfindung

[0001] Die Erfindung bezieht sich auf ein System und ein Verfahren zur Übertragung von Werten und insbesondere auf ein System und ein Verfahren, welche die Durchführung von Transaktionen mittels eines mobilen Kommunikationsgeräts ermöglichen, wie zum Beispiel bei der bargeldlosen Bezahlung für Produkte oder Dienstleistungen mit einem Mobilgerät an einer bestimmten Transaktionsstelle.

Stand der Technik

[0002] Systeme und Verfahren zur Bezahlung mit mobilen Geräten sind bekannt. Mobiltelefone werden zurzeit mit NFC-Chips (Englisch: near-field communication) und Firmware ausgestattet, welche sich bekanntlich für die automatische, kontaktlose und bargeldlose Zahlung eignen. Bei solchen NFC-Systemen geht man jedoch von einer umfangreichen Hardware- und Kommunikationsinfrastruktur aus. Jede Verkaufsstelle muss mit einem NFC Lesegerät ausgestattet sein, und nur derjenige, der über ein mit NFC ausgestattetes Gerät verfügt, kann von einem solchen System Gebrauch machen. Ferner sind die Kommunikationsmöglichkeiten zwischen dem Mobilgerät des Käufers und dem NFC-Gerät des Verkäufers durch die NFC-Technik bedingt, was zu einer erheblichen Inflexibilität des Systems führen kann.

Kurze Beschreibung der Erfindung

[0003] Die Erfindung sieht ein System gemäss Anspruch 1 und ein Verfahren gemäss Anspruch 11 vor. Die Erfindung wird anhand der beigelegten Zeichnungen beschrieben, in welchen:

Fig. 1	zeigt in einer schematischen Darstellung den Ablauf einer Bezahlung in einem erfindungsgemässen Verfahren bzw. System.
Fig. 2	zeigt in einer schematischen Darstellung den Ablauf einer Übertragung von Geld, Gutscheinen oder Werten zwischen zwei Wallets in einem erfindungsgemässen Verfahren bzw. System.
Fig. 3	zeigt in einer schematischen Darstellung den Ablauf vom Bezahlen auf Webseiten in einem erfindungsgemässen Verfahren bzw. System.
Fig. 4	zeigt in einer schematischen Darstellung den Ablauf einer Ladung von Gutscheinen, Werbegutscheinen oder andere Vergünstigungen in einem erfindungsgemässen Verfahren bzw. System.
Fig. 5	zeigt in einer schematischen Darstellung die Verwendung von Losen, Gutscheinen, Werbegeschenken oder Wettbewerbsteilnahme in einem erfindungsgemässen Verfahren bzw. System.
Fig. 6	zeigt in einer schematischen Darstellung das Verwalten von Wallets in einem erfindungsgemässen Verfahren bzw. System.
Fig. 7	zeigt in einer schematischen Darstellung den Ablauf einer Ladung von Geld in ein Wallet oder auf ein anderes Konto in einem erfindungsgemässen Verfahren bzw. System.

Detaillierte Beschreibung der Erfindung

[0004] Die Erfindung bezieht sich auf System und ein Verfahren zur sicheren Verwaltung und Übertragen von Werten ohne übermässigen Sicherheitsaufwand. Die Benutzer verfügen über ein oder mehrere Konten (Wallets). Diese sind entweder eigenständige Entitäten oder in Banken und Finanzinstitute integriert und damit Teil der normalen Konten dort.

[0005] Bei einer Bezahlung (Fig. 1) erstellt das Kassensystem (C) mit seinem eigenen Homeserver (H2), der auch in das Kassensystem C integriert sein kann (1 und 2 in Fig. 1), einen entsprechenden Invoice im System H2. H2 liefert dann einen Code zurück. Dieser Code, nachstehend auch Kennungscode genannt, kann verschiedene Gestalt annehmen. Er identifiziert den Homeserver H2 und den Invoice und enthält noch Sicherheitsmerkmale und Prüfsummen/Prüfmöglichkeiten. Der Code kann auf dem Server H2 mit einem Verfalldatum versehen sein. Er kann aber auch länger bleiben.

[0006] Das Kassensystem C zeigt den Code in Form einer möglichst einfach zu scannenden grafischen Reproduktion für den Kunden in einem Display (D in Fig. 1) oder einem Ausdruck an. Eine solche Reproduktion kann z.B. für einen QR-Code verwendet werden. Grundsätzlich kann aber jeder andere Barcode oder Darstellung gewählt werden, die einfach zu scannen bzw. mit einer Aufnahme danach wieder auszuwerten ist. Die angezeigte Darstellung wird mit dem mobilen Gerät (M) aufgenommen (4). Das mobile Gerät wertet den Code aus und schickt ihn (5) an seinen eigenen Homeserver (H1). Wenn ein Kunde mehrere Wallets oder mehrere Homeserver hat, so kann er einen auswählen. Dies muss vorgängig konfiguriert werden. Die Sicherheit erfolgt hier über die Verschlüsselung von (5) und die Anschlusskennung des Gerätes M. Zertifikate in der Anwendung und weitere Sicherheitsmerkmale (z.B. Passwörter) sind denkbar. Es ist auch möglich, dass erst anhand von Limiten (z.B. Betrag, Anzahl Transaktionen) weitere Sicherheitsmerkmale verlangt werden. H1 nimmt

dann Kontakt mit H2 (6) auf und lädt die Details herunter (7). Die Verbindungen (6, 7, 10 in Fig. 1) sind verschlüsselt. Die Details (insb. Betrag, Begünstigter) werden auf dem Display des mobilen Gerätes dargestellt (8). Der Kunde kann dann wählen, ob und wie er bezahlt. Dies teilt er H1 mit (9). Die Information wird über H2 (10) dem Kassiersystem mitgeteilt (11) und angezeigt (12). Im Hintergrund kann die Transaktion über die Bank B (a, b) stattfinden und H2 macht die Bestätigung an das Kassensystem C erst, wenn das Geld auf der Bank des Geschäfts angekommen ist. Es sind auch Transaktionen von Wallet zu Wallet möglich. Gutscheine im Wallet des Kunden können während der Schritte (6, 7 in Fig. 1) geprüft werden. Diese werden in (8) zur Verwendung vorgeschlagen. Über Eingaben auf M kann der Kunde diese bestätigen. Die Kontrolle über die Ansicht und Verwendung liegt einzig beim Kunden (Informationen und Verarbeitung in H1 und M). Eine automatische Verarbeitung mit H2 ist möglich, hat dann aber die Form eines Cookies und muss vom Kunden explizit bestätigt werden (in den Einstellungen).

[0007] Mit dem System ist es auch möglich, Guthaben und Gutscheine auszutauschen. Das kann über die Einheiten C und D in Fig. 1 geschehen. Alternativ können so geladene Geschenkgutscheine, Guthaben oder andere Werte zwischen zwei Benutzern generell ausgetauscht werden (Fig. 2). Der eine Benutzer lädt (1, 2 in Fig. 2) von seinem Wallet auf Homeserver H1 eine entsprechende Kennung herunter und lässt diese als Kennungscode (etwa Barcode, QR-Code oder in anderer geeigneter Weise) auf dem Display seines mobilen Geräts (Ml) darstellen. Der zweite Benutzer fotografiert (3 in Fig. 2) mit seinem Gerät (M2) den Kennungscode. Die Kennung wird dechiffriert und die notwendigen Daten werden über den normalen Weg (4, 5, 6, 7 in Fig. 2) geladen und angezeigt. Der Benutzer bestätigt dann den Transfer. Dieser kann über H2, H1 auch auf dem Gerät (Ml) des Benutzers dargestellt werden. Dieser Teil ist auf der Abbildung nicht eingezeichnet. Dieser Ablauf ist als Transaktion aufgebaut, da der Wert dann nicht mehr im Wallet von H1, sondern nur noch in dem von H2 ist. Solche Transaktionen sind üblicherweise zeitlich limitiert, um die Sicherheit zu erhöhen.

[0008] Das System lässt sich für verschiedene Währungen, auch künstliche und Mikropayments verwenden. Es kann ebenfalls für die Bezahlung über das Web verwendet werden. Der Ablauf ist in Fig. 3 dargestellt. Wenn der Webserver (W1) eine Bezahlung ausgeführt haben will, dann erstellt er die notwendige Transaktion im Homeserver (H2) (1, 2 in Fig. 3). Er übermittelt die zurückgelieferte Kennung an den Benutzer auf dem Gerät (D). Die Darstellung als Kennungscode (Barcode, QR-Code usw.) wird vom Benutzer mit seinem mobilen Gerät (M) fotografiert. Die Kennung wird entschlüsselt. Über seinen eigenen Homeserver (H1) (5) werden die Transaktionsinformationen von H2 geholt (6, 7 in Fig. 3). Auch diese Kommunikation kann mehrere Schritte umfassen, wenn die Homeserver H1, H2 noch Elemente verhandeln müssen. Die Anzeige erfolgt dann auf dem mobilen Gerät (8). Der Benutzer wählt dann eine Aktion aus. Die Bezahlung erfolgt dann über H1 (9) auf H2 (2). Entweder handelt es sich bei (9) wieder um eine Transaktion zwischen Wallets oder Geld wird wie auch bei den anderen hier beschriebenen Bezahlungen über eine normale Bank-, Kreditkarten, Paypal-Verbindung bezahlt. Es obliegt den Einstellungen der Homeserver, ob die Transaktion vorher abgeschlossen wird. Die Bezahlung wird dem Webserver (W) gemeldet, der danach z.B. den Download freigibt und auch auf dem Display anzeigt (12 in Fig. 3). Der Abschluss der Transaktion kann auch auf dem mobilen Gerät M noch angezeigt werden.

[0009] Das System kann auch für Werbung, Coupons, Rabatte, Gutscheine verwendet werden (Fig. 5). Über den Homeserver H1 werden die notwendigen Einträge im Wallet erstellt, die dazugehörige Kennung wird zurückgeliefert oder direkt druckfertig dargestellt (1 in Fig. 5). Auch hier handelt es sich üblicherweise um einen 2-dimensionen Barcode. Andere Darstellungen sind aber möglich, solange sie sich einfach scannen lassen. Auf der Anzeige, dem Produkt oder Medium wird der Barcode dargestellt (es kann sich auch um Fernsehen, Internet, Banner usw. handeln). Der Benutzer fotografiert den Code (2 in Fig. 5) mit seinem mobilen Gerät (M). Die Kennung wird ausgelesen. Über seinen Homeserver (H2, 3) wird die Detailinformation bei H1 abgeholt (4, 5) und dem Benutzer auf seinem Gerät angezeigt (6). Der Benutzer bestätigt dann entweder die Integration des Gutscheins, Guthabens, Rabatt-Coupons in sein Wallet oder verwirft diese (7 in Fig. 5). Der Inhalt der Werbung kann zeitlich oder anderweitig limitiert sein (z.B. Produkte, Orte, Läden, Einkaufssumme). Sie kann ein Rabatt sein, eine Gutschrift oder direkt in Währung konvertierbar. Es ist auch möglich Punktesysteme von Firmen damit abzubilden.

[0010] Der Benutzer kann sein Wallet oder seine Wallets sowohl mit dem mobilen Gerät (M) wie auch von einer normalen Arbeitsstation oder einem speziellen Anschluss (G) verwalten (Fig. 6). Üblicherweise geschieht diese Verwaltung über eine sichere Verbindung (1, 2 in Fig. 6).

[0011] Im Wallet sind die Daten gespeichert. Es werden detaillierte Logs geführt.

[0012] Das Wallet kann direkt Guthaben und Währungen aufnehmen. Dies geschieht entweder über die Bank oder über Transaktionen mit anderen Benutzern. Ein Aufladen ist auch an Geldautomaten oder Shops möglich (Fig. 7). An der ATM läuft der normale Prozess bis zur Geldausgabe, in einem Shop muss das Geld über eine Karte oder bar gegeben werden (ATM). Wenn dann eine Ausgabe als Konto im Wallet gewünscht wird, so teilt die ATM das dem Bankserver B (der entweder selbst ein Homeserver ist, oder einen solchen verwendet) mit. Der Homeserver der Bank generiert die Transaktion und die Kennung. Die Kennung wird an ATM übermittelt (2 in Fig. 7) und in geeigneter Form dargestellt. Der Benutzer fotografiert die Kennung mit seinem mobilen Gerät (3) und leitet die Anfrage dann an seinen Homeserver (H4) weiter. Dieser benutzt die Kennung, um die relevanten Angaben vom Server B zu beziehen (5, 6). Diese werden dem Benutzer angezeigt (7). Wenn die Transaktion für den Benutzer stimmt, so löst er sie aus (8). Das Guthaben wird dann transferiert (9) und das Resultat auf dem Display der ATM angezeigt (10). Solche Kennungen sind üblicherweise nur kurz gültig, um die Sicherheit zu erhöhen.

[0013] Es ist möglich, in den Wallets mehrere Währungen zu führen. Es ist auch möglich, «Spiel»währungen oder unternehmensspezifische Währungen zu führen. Die Transaktionen können limitiert sein.

[0014] Es ist für einen Benutzer möglich, verschiedene Wallets auf verschiedenen Homeservern zu haben.

[0015] Es ist möglich, dass das Wallet eher Rechnungen verwaltet, die mit einem normalen eBanking, bzw. einer eBanking-Schnittstelle bezahlt werden. Dann beschreiben die oben genannten Abläufe den Fluss der Rechnung und die Anerkennung der Forderung.

[0016] Das System kann auch für vereinfachte Bearbeitung von Papierrechnungen verwendet werden, indem diese eine entsprechende grafische Kennung aufweisen. Die Details werden dann nach der Aufnahme mit dem mobilen Gerät (M) vom entsprechenden Homeserver abgeholt und auf dem mobilen Gerät angezeigt und dem eBankingsystem (oder Homeserver) weitergeleitet.

[0017] Die Sicherheit basiert u.a. auf dem der Anschlusskennung des mobilen Gerätes, des Weiteren auf der sicheren Verbindung aller Komponenten. Über die Kennzeichnungen lassen sich auch Zertifikate und Schlüssel austauschen. Die Applikationen auf M können selber Zertifikate beinhalten und generieren. Die Homeserver besitzen starke Zertifikate. Eine koordinierende Stelle weist alle Adressen und die öffentlichen Schlüssel der Homeserver aus. Diese wird auch angefragt, wenn der Anschluss eines Homeservers H2 (als Teil der Kennung), dem Homeserver H1 nicht bekannt ist. Der öffentliche Schlüssel dieser koordinierenden Server ist Teil jeder Anwendung des Systems. Die Kennung kann auch für zukünftige Erweiterungen eine Versionsnummer erhalten.

[0018] Die Kennung soll möglichst kurz gehalten werden, so dass der entsprechend grafisch dargestellte Code auch mit leistungsschwachen Kameras aufgenommen werden kann.

Patentansprüche

1. System zur Durchführung einer Transaktion an einer Transaktionsstelle mittels eines mit einer optischen Aufnahmeeinrichtung ausgestatteten Mobilgeräts (M) eines Benutzers, wobei das System aufweist:
einen ersten Server (H1), auf welchem mindestens ein Eintrag in einem Benutzerkonto des Benutzers, nachstehend Wallet genannt, abspeicherbar ist; und
einen zweiten Server (H2), mittels welchem ein Kennungscode erstellbar ist, wobei der Kennungscode Transaktionsinformationen der genannten Transaktion umfasst; und
eine erste verschlüsselte Kommunikationsverbindung (5, 8, 9 in Fig. 1) zur Übertragung der Transaktionsinformationen vom Mobilgerät (M) an den ersten Server (H1); gekennzeichnet durch
ein Reproduktionsmittel (D) zur grafischen Darstellung des Kennungscodes an der Transaktionsstelle; und
eine zweite verschlüsselte Kommunikationsverbindung (1, 2 in Fig. 1) zur Übertragung des Kennungscodes vom zweiten Server (H2 in Fig. 1) an das Reproduktionsmittel;
wobei der erste Server (H1), der zweite Server (H2) und das Reproduktionsmittel (D) derart konfiguriert sind, dass der an der Transaktionsstelle dargestellte Kennungscode mittels der optischen Aufnahmeeinrichtung aufnehmbar und an den ersten Server (H1) übertragbar ist;
und wobei der erste Server (H1) derart konfiguriert ist, dass die, dem vom Mobilgerät (M) empfangenen Kennungscode entsprechenden Transaktionsinformationen als der genannte Eintrag in das genannte Wallet abspeicherbar sind.
2. System gemäss Anspruch 1, wobei das Reproduktionsmittel (D) derart konfiguriert ist, um den Kennungscode als ein- oder zwei-dimensionaler Barcode darstellen zu können.
3. System gemäss Anspruch 1 oder 2, wobei die Transaktionsinformationen Informationen zu einer Übertragung von Werten umfasst;
wobei der erste Server (H1) derart konfiguriert ist, um mehrere Wallets abspeichern zu können; und
wobei der erste Server (H1) derart konfiguriert ist, dass auf Empfang der Transaktionsinformationen vom Mobilgerät (M), die Übertragung von Werten zwischen zwei der mehreren Wallets durchführbar ist.
4. System gemäss einem der vorhergehenden Ansprüche, wobei der erste Server (H1) und die erste Kommunikationsverbindung (5, 8 in Fig. 1) derart konfiguriert sind, dass das Wallet über das Mobilgerät (M) verwaltbar ist.
5. System gemäss einem der vorhergehenden Ansprüche, wobei das Reproduktionsmittel (D) einen Ausdruck oder ein elektronisches Anzeigemedium umfasst, und wobei das System derart konfiguriert ist, um die genannte Darstellung des Kennungscodes zeitlich oder geografisch limitieren zu können.
6. System gemäss einem der vorhergehenden Ansprüche, wobei der erste Server (H1) derart konfiguriert ist, dass eine vorbestimmte Obergrenze der Anzahl Transaktionen, eine vorbestimmte Obergrenze eines Transaktionsbetrags und/oder eine vorbestimmte Obergrenze eines Gesamtbetrags pro Zeiteinheit einstellbar sind.
7. System gemäss einem der vorhergehenden Ansprüche, welches eine dritte Kommunikationsverbindung (a, b) aufweist, wodurch das Wallet an ein Banking-, eBanking- oder Bezahlsystem anschliessbar ist.
8. Verfahren zur Durchführung einer Transaktion an einer Transaktionsstelle mittels eines mit einer optischen Aufnahmeeinrichtung ausgestatteten Mobilgeräts (M) eines Benutzers, wobei das Verfahren aufweist:

einen ersten Schritt, in welchem ein Benutzerkonto des Benutzers, nachstehend Wallet genannt, an einem ersten Server (H1) bereitgestellt wird;
einen zweiten Schritt, in welchem ein Kennungscode an einem zweiten Server (H2) erstellt wird, wobei der Kennungscode eine Transaktionsinformationen der genannten Transaktion umfasst;
einen dritten Schritt, in welchem ein Reproduktionsmittel zur grafischen Darstellung des Kennungscodes an der Transaktionsstelle bereitgestellt wird;
einen vierten Schritt, in welchem der Kennungscode über eine zweite verschlüsselte Kommunikationsverbindung (2, 3) vom zweiten Server (H2) an das Reproduktionsmittel (D) übertragen und an der Transaktionsstelle grafisch dargestellt wird;
einen fünften Schritt, in welchem der an der Transaktionsstelle dargestellte Kennungscode mittels der Aufnahmeeinrichtung des Mobilgeräts (M) des Benutzers aufgenommen wird;
einen sechsten Schritt, in welchem die Transaktionsinformationen über eine erste verschlüsselte Kommunikationsverbindung (5, 8) vom Mobilgerät (M) an den ersten Server (H1) übertragen werden;
einen siebten Schritt, in welchem die, dem vom Mobilgerät (M) empfangenen Kennungscode entsprechenden Transaktionsinformationen als der genannte Eintrag im genannten Wallet abgespeichert werden.

9. Verfahren gemäss Anspruch 8, wobei der Kennungscode als ein- oder zwei-dimensionaler Barcode dargestellt wird.

10. Verfahren gemäss Anspruch 8 oder 9, wobei die Transaktionsinformationen Informationen zu einer Übertragung von Werten umfasst; wobei mehrere Wallets am ersten Server abgespeichert werden; und wobei nach Empfang der Transaktionsinformationen vom Mobilgerät, die Übertragung von Werten zwischen zwei der mehreren Wallets durchgeführt wird.

11. Verfahren gemäss einem der Ansprüche 8 bis 10, welches einen Verwaltungsschritt umfasst, wobei das Wallet über das Mobilgerät (M) verwaltet wird.

12. Verfahren gemäss einem der Ansprüche 8 bis 11, wobei das Reproduktionsmittel (D) einen Ausdruck oder ein elektronisches Anzeigemedium umfasst, und wobei die genannte Darstellung des Kennungscodes zeitlich oder geografisch limitiert wird.

13. Verfahren gemäss einem der Ansprüche 8 bis 12, welches einen achten Schritt umfasst, in welchem eine vorbestimmte Obergrenze der Anzahl Transaktionen, eine vorbestimmte Obergrenze eines Transaktionsbetrags und/oder eine vorbestimmte Obergrenze eines Gesamtbetrags pro Zeiteinheit eingestellt werden.

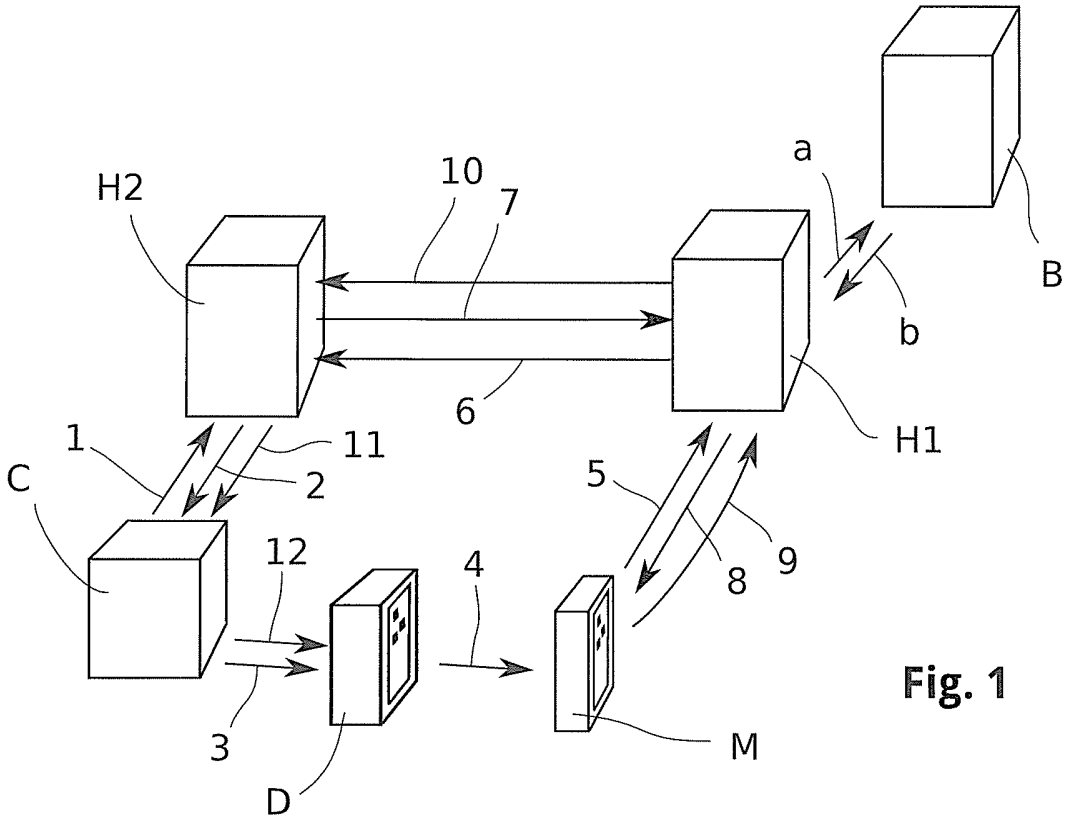


Fig. 1

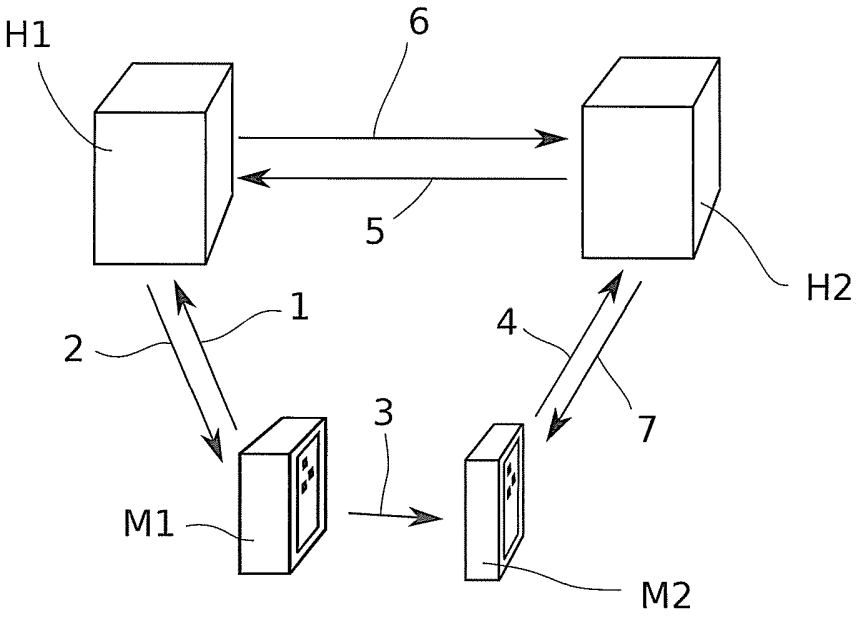


Fig. 2

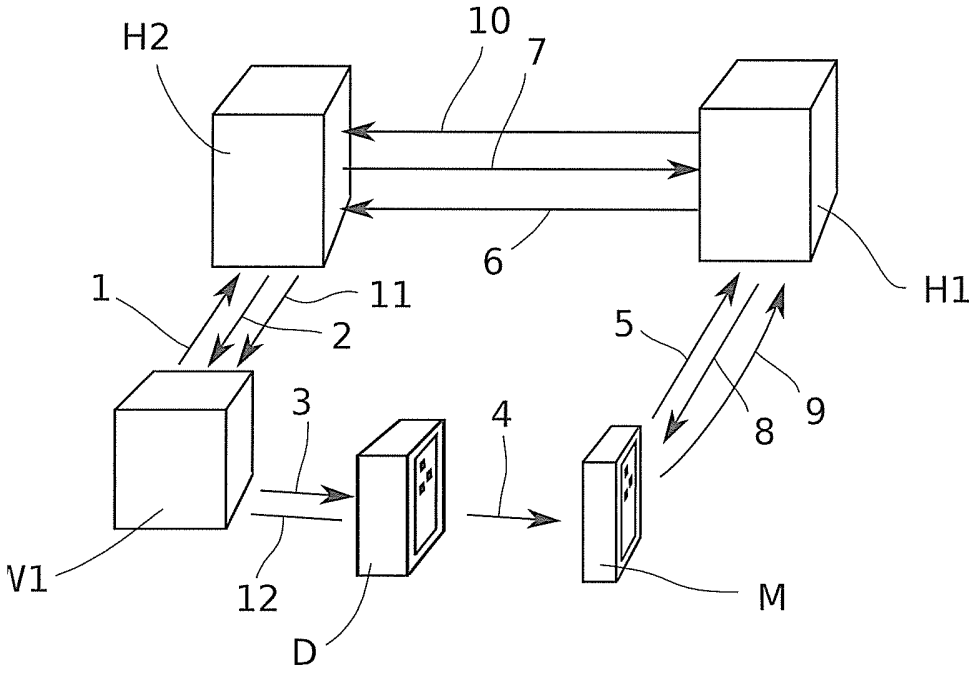


Fig. 3

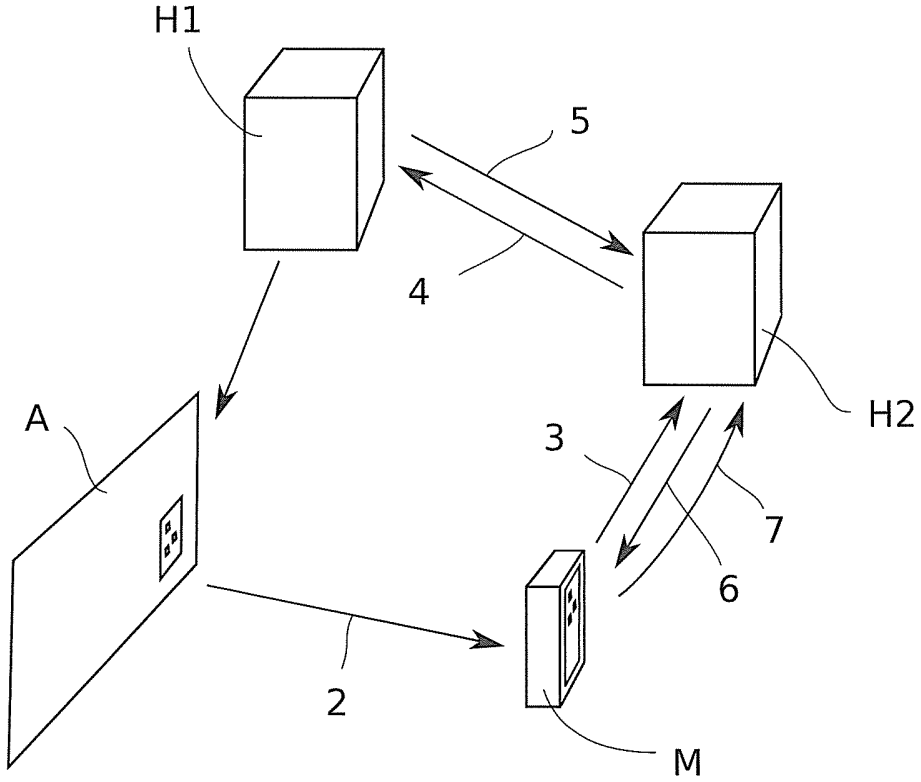


Fig. 4

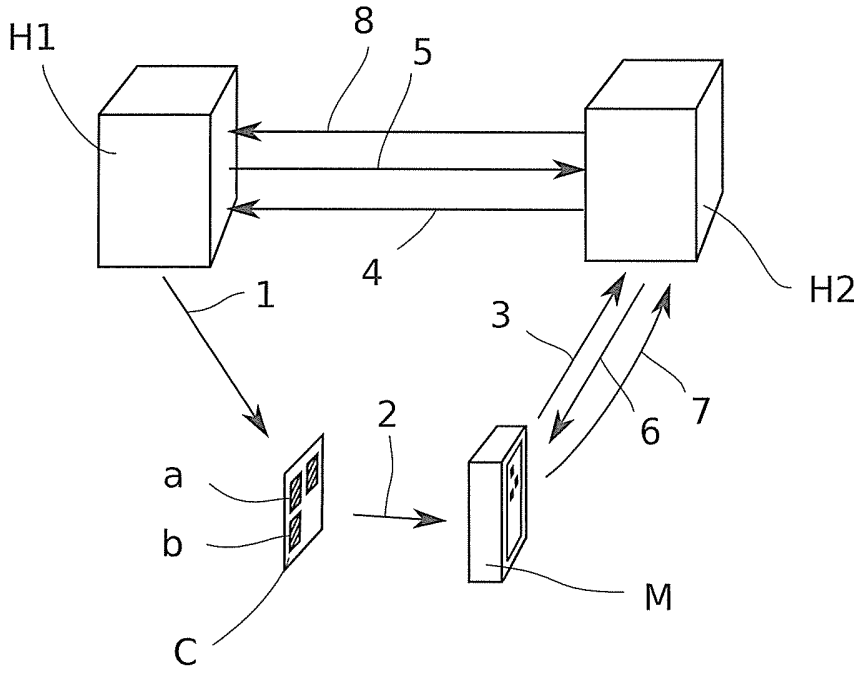


Fig. 5

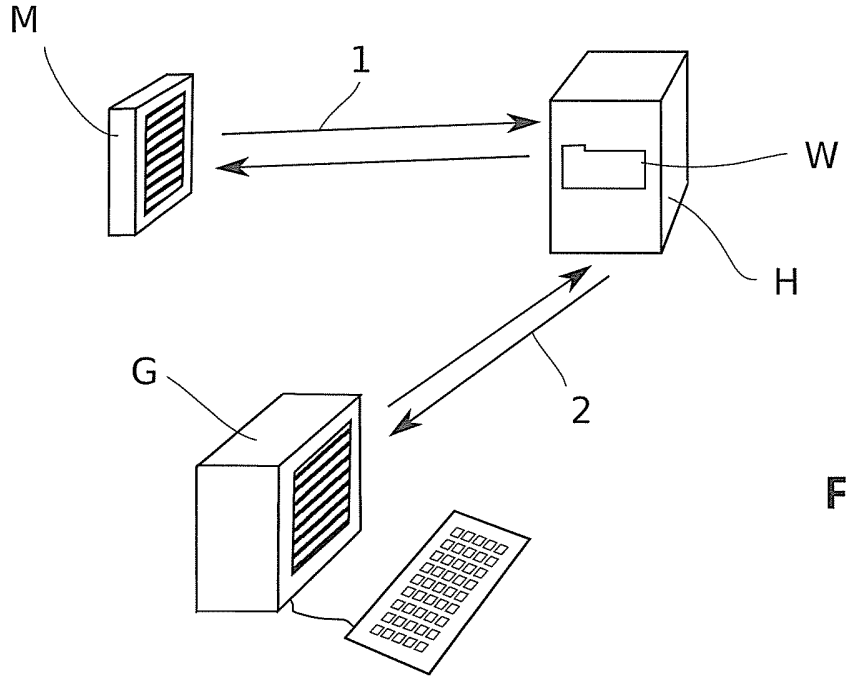


Fig. 6

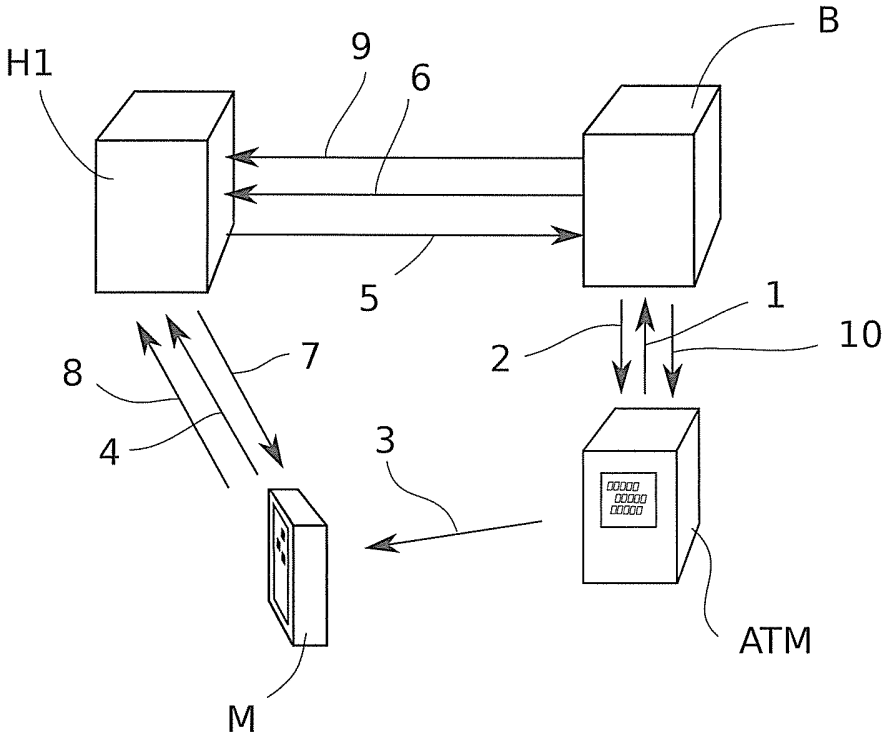


Fig. 7