(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 115 034 A1** 2021.12.09

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 115 034.2**
(22) Anmeldetag: **05.06.2020**
(43) Offenlegungstag: **09.12.2021**

(51) Int Cl.: ***G06Q 20/30*** (2012.01)
G06F 21/62 (2013.01)
G07D 7/00 (2016.01)
B42D 25/29 (2014.01)
B42D 25/305 (2014.01)

(71) Anmelder:
Bundesdruckerei GmbH, 10969 Berlin, DE

(74) Vertreter:
Richardt Patentanwälte PartG mbB, 65185 Wiesbaden, DE

(72) Erfinder:
Peters, Florian, Dr., 10437 Berlin, DE; Sauter, Dieter-Heinrich, Dr., 81379 München, DE

(56) Ermittelter Stand der Technik:

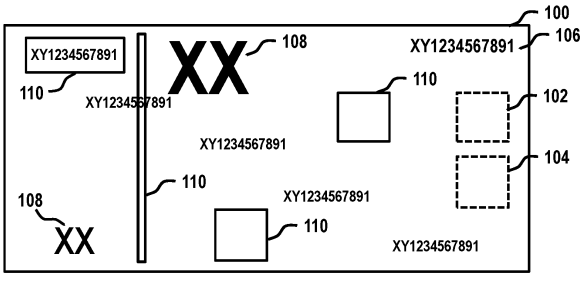
DE	**101 47 140**	**A1**
DE	**197 18 547**	**A1**
GB	**2 528 486**	**A**
US	**2016 / 0 071 094**	**A1**
US	**2019 / 0 034 912**	**A1**

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Banknote mit Prozessor**

(57) Zusammenfassung: Die Erfindung betrifft eine Banknote (100) mit einem Prozessor (124) und einem Speicher (120). In dem Speicher (120) des Sicherheitselements (102) ist eine Identifikationsnummer (116) der Banknote (100) gespeichert, welche ein von einer die Banknote (100) ausgebenden Zentralbank (220) verwaltetes und der entsprechenden Banknote (100) individuell zugeordnetes anonymes Banknotenkonto identifiziert. In einem geschützten Speicherbereich (122) des Speichers (120) ist ein banknotenindividueller kryptographischer Schlüssel (118) gespeichert. Ein mit der Banknote (100) ausgeführtes Zahlungsverfahren umfasst:
• Empfangen einer Zahlungsanfrage für eine Zahlung mit der Banknote (100),
• Erzeugen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote (100), wobei das Kryptogramm aus der Identifikationsnummer (116) der Banknote (100) und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels (118) erzeugt wird,
• Senden einer das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung.



Beschreibung

[0001] Die Erfindung betrifft eine Banknote sowie Verfahren zum Ausstellen, Verwenden und Ersetzen von Banknoten. Ferner betrifft die Erfindung ein Verfahren zur Zahlungsabwicklung unter Verwenden eines Terminals.

[0002] Im Zuge der zunehmenden Digitalisierung rücken heutzutage mehr und mehr bargeldlose Zahlungsinstrumente in den Vordergrund, insbesondere basierend auf elektronischen Verfahren zur Zahlungsabwicklung. Im bargeldlosen Zahlungsverkehr erfolgt ein Transfer von Zahlungsmitteln, ohne dass dabei Bargeld transferiert wird. Bei Barzahlungen wird Bargeld, d.h. Banknoten oder Münzen, zwischen Zahlungspflichtigem und Zahlungsempfänger ausgetauscht, während es bei einer bargeldlosen Zahlung nicht zu einem solchen Austausch von Bargeld kommt.

[0003] Bargeld hat beispielsweise den Vorteil, dass es für jedermann verfügbar ist und schnell sowie überall eingesetzt werden kann. So ist beispielsweise für eine bargeldbasierte Zahlungsabwicklung kein Bankkonto erforderlich. Zudem wird Bargeld von den Besitzern oftmals als Wertaufbewahrungsmittel geschätzt.

[0004] Bargeldlose Zahlungsverfahren haben demgegenüber beispielsweise den Vorteil, dass sie eine effiziente Zahlungsabwicklung ermöglichen, selbst wenn sich Zahlungspflichtiger und Zahlungsempfänger an entfernten Orten aufhalten, wie es beispielsweise bei Einkäufen über das Internet der Fall ist. Dies können bekannte Banknoten nicht leisten.

[0005] Der Erfindung liegt daher die Aufgabe zugrunde, eine verbesserte Banknote zu schaffen.

[0006] Die der Erfindung zugrundeliegende Aufgabe wird jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

[0007] Ausführungsformen umfassen eine Banknote. Die Banknote umfasst ein Sicherheitselement mit einem Prozessor und einem Speicher mit Programminstruktionen. In dem Speicher des Sicherheitselements ist eine Identifikationsnummer der Banknote gespeichert, welche ein von einer die Banknote ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote individuell zugeordnetes anonymes Banknotenkonto identifiziert. In einem geschützten Speicherbereich des Speichers des Sicherheitselements ist ein banknotenindividueller kryptographischer Schlüssel gespeichert.

[0008] Der Prozessor ist dazu konfiguriert bei Ausführen der Programminstruktionen ein Zahlungsverfahren mit der Banknote auszuführen. Das Zahlungsverfahren umfasst:

- Empfangen einer Zahlungsanfrage für eine Zahlung mit der Banknote,
- Erzeugen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote, wobei das Kryptogramm aus der Identifikationsnummer der Banknote und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt wird,
- Senden einer das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung.

[0009] Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer. Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe der Identifikationsnummer. Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe eines der Banknote zugeordneten initialen Nominalwerts.

[0010] Ausführungsformen können den Vorteil haben, dass die Banknote nicht nur als Bargeldzahlungsmittel im üblichen Sinne verwendet werden verwendet kann, sondern zusätzlich auch eine bargeldlose Zahlung mit der Banknote ausgeführt werden kann. Bei einer Verwendung als Bargeldzahlungsmittel im üblichen Sinne wird die Banknote im Zuge des Zahlungsabwicklung von dem Zahlungspflichtigen an den Zahlungsempfänger übergeben oder der Zahlungsempfänger übergibt die entsprechende Banknote als Wechselgeld im Zuge der Zahlungsabwicklung dem Zahlungspflichtigen. Mit der Übergabe der Banknote geht das Eigentum an der Banknote von dem Übergeber an den Empfänger über. Mit dem Eigentum an der Banknote geht auch das Eigentum an dem aktuellen Nominalwert der Banknote, d.h. dem dem Banknotenkonto der Banknote zugeordneten Nominalwert, an den Empfänger über.

[0011] Bei einer Verwendung für eine bargeldlose Zahlung, d.h. ohne Übergabe der Banknote bzw. Übergang des Eigentums an der Banknote, erfolgt die Zahlung durch ein Bereitstellen eines zahlungsindividuellen Kryptogramms durch die Banknote. Dieses Kryptogramm autorisiert eine Transaktion, bei welcher der zu zahlende Betrag von dem Banknotenkonto der Banknote an ein Konto des Zahlungsempfängers transferiert wird.

[0012] Beispielsweise definiert sich die im Umlauf befindliche und sowohl bargeldbasiert als auch bargeldlos transferierbare Geldmenge durch die Geldmenge bzw. der Summe der Nominalwerte, welche Banknotenkonten von Banknoten zugeordnet

sind. Beispielsweise bleibt die im Umlauf befindliche Geldmenge gleich, falls die im Umlauf befindlichen Banknoten beibehalten werden. Das bedeutet beispielsweise, dass im Umlauf befindlichen Banknoten gleichbleiben können, sich aber in Folge von Transaktionen die den individuellen Banknoten zugeordneten Nominalwerte ändern können. Beispielsweise wäre es auch möglich die den Banknoten zugeordnete Geldmenge ohne die im Umlauf befindlichen Banknoten zu ändern, falls die Zentralbank Zahlungstransfers von Banknotenkonten zu anderen Konten, etwa in andere Systeme, wie z.B. dem GIRO SEPA System, und umgekehrt zulässt.

[0013] Da weder die Banknote noch deren Banknotenkonto einer rechtlichen oder natürlichen Peron zugeordnet sind, ermöglich die Banknote beispielsweise sowohl bargeldbasierte als auch bargeldlose anonyme Zahlungen, wie sie aktuell nur mit Bargeld möglich sind. Um Missbrauch vorzubeugen könnten beispielsweise zusätzlich Beschränkungen implementiert werden, welche transferierbare Geldmengen limitieren und/oder ab bestimmten Geldbeträgen zusätzliche Prüfmechanismen vorsehen. Entsprechende Prüfmechanismen könnten beispielsweise eine Freigabe der Transaktion durch die Zentralbank auf Basis einer Prüfung zusätzlicher als notwendig festgelegter Angaben zu der entsprechenden Transaktion erfordern.

[0014] Die Banknote und damit deren Nominalwert gemäß Banknotenkonto kann beispielsweise durch händische physische Übergabe weitergegeben werden, d.h. eine digitale Währung kann übergeben werden. Dafür ist beispielsweise kein persönliches Konto des Nutzers der Banknote, d.h. ein einer rechtlichen oder natürlichen Person zugeordnetes Konto, notwendig. Es kann beispielsweise Material und Aufwand gespart werden durch Reduzieren der rein analogen Währung. Insbesondere kann der Aufwand beim physischen Transfer und Transport von Banknoten reduziert werden. Eine solche Banknote kann beispielsweise aufgewertet und zur direkten Kontaktloszahlung genutzt werden, ohne oder nur mit beschränkter Kontrolle oder Nachverfolgen, da eine individuelle Banknote wie im Falle klassischen Bargelds jederzeit weitergeben werden kann.

[0015] Beispielsweise ist der aktuelle Nominalwert der Banknote zusätzlich in dem Speicher des Sicherheitselements hinterlegt. Ausschlaggeben für den tatsächlichen Nominalwert der Banknote ist deren Nominalwert gemäß Banknotenkonto. Beispielsweise kann der in der Banknote hinterlegte Nominalwert zu einer offline Bestimmung des aktuellen Nominalwerts verwendet werden. Beispielsweise wird der in der Banknote hinterlegte Nominalwert aktualisiert, wenn zum Abschluss einer Transaktion eine von der Zentralbank signierte Transaktionsbestätigung an die Banknote weitergeleitet wird. Beispielsweise verfügt das Sicherheitselement über einen Signaturprüfschlüssel zum Prüfen digitaler Signaturen der Zentralbank.

[0016] Der tatsächliche Nominalwert einer Banknote wird beispielsweise alleine von dem Nominalwert bzw. dem Guthaben des Banknotenkontos bestimmt, welches der Banknote zugeordnet ist. Um über das Guthaben des Banknotenkontos und damit den Nominalwert der Banknote verfügen zu können, ist der Besitz einer dem entsprechenden Banknotenkonto echten Banknote mit einem banknotenindividuellen kryptographischen Schlüssel notwendig.

[0017] Beispielsweise kann auf Basis des ermittelten aktuelle Nominalwerts entschieden werden, ob eine Bargeldzahlung oder eine bargeldlose Zahlung mit der Banknote erfolgen soll. Ist der aktuelle Nominalwert identisch mit dem zu zahlenden Betrag, erfolgt beispielsweise eine Bargeldzahlung, bei welcher die Banknote an den Zahlungsempfänger übergeben wird und das Eigentum an dieser an den Zahlungsempfänger übergeht. Ist der aktuelle Nominalwert größer als der zu zahlenden Betrag, erfolgt beispielsweise eine Bargeldlosezahlung. Bei der Bargeldlosezahlung wird beispielsweise eine entsprechende Zahlungsanfrage an die Banknote gesendet für eine Zahlung in Form einer Transaktion eines zu zahlenden Betrags von dem Banknotenkonto der Banknote an ein Konto, beispielsweise Banknotenkonto, eines Zahlungsempfängers. Die Banknote kann diese Transaktion mit einem zahlungsindividuellen Kryptogramm autorisieren.

[0018] Ist der aktuelle Nominalwert größer als der zu zahlenden Betrag, wäre es ebenso möglich, dass eine Bargeldzahlung erfolgt und der überzählige Betrag als Wechselgeld, beispielsweise in Form von Bargeld, etwa Banknoten mit passendem Nominalwert, von dem Zahlungsempfänger zurückgezahlt wird.

[0019] Beispielsweise kann der aktuelle Nominalwert jeden positiven Wert einschließlich Null annehmen. Das Banknotenkonto kann mithin beispielsweise nicht überzogen werden. Beispielsweise kann der aktuelle Nominalwert jeden Wert zwischen Null und einem vorgegebene Maximalnominalwert annehmen. Beispielsweise kann der aktuelle Nominalwert jeden Wert größer oder gleich einem vorgegebene Mindestnominalwert annehmen. Beispielsweise kann der aktuelle Nominalwert jeden Wert von einschließlich einem vorgegebene Mindestnominalwert bis einschließlich einem vorgegebene Maximalnominalwert annehmen.

[0020] Beispielsweise kann der Nominalwert der Banknote einen garantierten Mindestnominalwert und einen variablen Zusatznominalwertanteil umfassen. Der Mindestnominalwert kann beispielsweise nur in Form einer Bargeldzahlung mit Übergabe der

Banknote gezahlt werden, während der variable Zusatznominalwertanteil im Zuge einer bargeldbasierten oder bargeldlosen Zahlungsabwicklung verwendet werden kann. Mit anderen Worten könnten mit der Banknote nur bargeldlose Zahlungen erfolgen, bei welchen der verbleidende Nominalwert der Banknote größer oder gleich dem Mindestnominalwert ist. Soll mit der Banknote ein Betrag gezahlt werden, welcher in einem verbleidenden Nominalwert resultieren würde, der kleiner dem Mindestnominalwert wäre, wird eine bargeldlose Zahlung unter Verwendung des Banknotenkontos beispielsweise blockiert. Mithin ist beispielsweise ein Mindestguthaben des Banknotenkontos in Form des garantierten Mindestnominalwerts festgelegt. In diesem Fall muss beispielsweise eine bargeldbasierte Zahlung erfolgen, bei welcher die Banknote übergeben wird. Ist der aktuelle Nominalwert der Banknote größer als der zu zahlende Betrag, so kann der Differenzbetrag beispielsweise in Form von Wechselgeld durch den Zahlungsempfänger rückerstattet werden.

[0021] Beispielsweise ist der initiale Nominalwert für die Banknote bzw. das Startguthaben des Banknotenkontos in einem Register der Zentralbank eingetragen und wird von dieser in einem von ihr verwalteten Zahlungssystem verbucht. Beispielsweise transferiert die Zentralbank im Zuge der Initialisierung der Banknote das Startguthaben von einem Konto der Zentralbank auf das Banknotenkonto der zu initialisierenden Banknote.

[0022] Beispielsweise sind die visuelle Gestaltung, die eingebrachten Sicherheitsmerkmale und/oder das Format der Banknote abhängig von deren initialem Nominalwert. Somit unterscheiden sich Banknoten mit unterschiedlichem initialem Nominalwert beispielsweise hinsichtlich ihrer visuellen Gestaltung, der eingebrachten Sicherheitsmerkmale und/oder des Formats voneinander. Banknoten mit identischem initialem Nominalwert weisen beispielsweise abgesehen von ein oder mehreren banknotenindividuellen Angaben, wie etwa Seriennummer, Angaben zum Ausstellungjahr etc., eine identische visuelle Gestaltung, identische Sicherheitsmerkmale und/oder Formate auf.

[0023] Beispielsweise umfasst die Banknote eine visuelle Angabe des Mindestnominalwerts. Beispielsweise ist der Mindestnominalwert für die Banknote bzw. das für das Banknotenkonto festgelegte Mindestguthaben in einem Register der Zentralbank eingetragen. Beispielsweise sind die visuelle Gestaltung, die eingebrachten Sicherheitsmerkmale und/oder das Format der Banknote abhängig von deren Mindestnominalwert. Somit unterscheiden sich Banknoten mit unterschiedlichen Mindestnominalwerten beispielsweise hinsichtlich ihrer visuellen Gestaltung, der eingebrachten Sicherheitsmerkmale und/oder des Formats voneinander. Banknoten mit identischen Mindestnominalwerten weisen beispielsweise abgesehen von ein oder mehreren banknotenindividuellen Angaben, wie etwa Seriennummer, Angaben zum Ausstellungjahr etc., eine identische visuelle Gestaltung, identische Sicherheitsmerkmale und/oder Formate auf.

[0024] Beispielsweise handelt es sich bei dem der Banknote zugeordneten initialen Nominalwert, welchen die Banknote als visuelle Angabe umfasst, um den gesamten Nominalwert, welcher der Banknote im Zuge ihrer Initialisierung von der Zentralbank auf das der Banknote zugeordnete Banknotenkonto transferiert wird. Beispielsweise handelt es sich bei dem gesamten der Banknote initial zugeordneten Nominalwert um den garantierten Mindestnominalwert und einen initialen Zusatznominalwertanteil. Der Zusatznominalwertanteil ist beispielsweise variable in Abhängigkeit von den Transaktionen, welche von dem und auf das Banknotenkonto der Banknote ausgeführt werden. Beispielsweise handelt es sich bei dem visuell angegebenen initialen Nominalwert um einen Anteil des gesamten Nominalwerts, welcher der Banknote im Zuge ihrer Initialisierung als Startguthaben auf dem Banknotenkonto zugeordnet wird. Beispielsweise handelt es sich bei dem entsprechenden Anteil um den Mindestnominalwert, wobei der tatsächliche gesamte Nominalwert initial größer sein kann, d.h. einen initialen Zusatznominalwertanteil umfassen kann. Beispielsweise ist der gesamte Nominalwert, welcher der Banknote im Zuge ihrer Initialisierung auf das Banknotenkonto transferiert wird, ein Mindestnominalwert der Banknote, welcher beispielsweise visuell auf der Banknote angegeben ist. In diesem Fall handelt es sich bei der visuellen Angabe des initialen Nominalwerts beispielsweise zugleich um eine visuelle Angabe des Mindestnominalwerts der Banknote. Beispielsweise unterscheidet sich der Mindestnominalwert von dem initialen Nominalwert. In diesem Fall umfasst die Banknote beispielsweise eine visuelle Angabe des Mindestnominalwerts zusätzlich zu der visuellen Angabe des initialen Nominalwerts.

[0025] Ein Hinzufügen eines variablen Zusatznominalwertanteils oder eine Erhöhung eines bestehenden variablen Zusatznominalwertanteils erfolgt beispielsweise durch eine Transaktion eines entsprechenden Betrags auf das Banknotenkonto der Banknote. Die Transaktion kann von einem anderen Konto stammen, beispielsweise einem Banknotenkonto einer anderen Banknote oder einem Konto der Zentralbank. Beispielsweise ist variable Zusatznominalwertanteil unbegrenzt erhöhbar. Beispielsweise ist der variable Zusatznominalwertanteil in Abhängigkeit von dem Mindestnominalwert und/oder dem initialen Nominalwert erhöhbar. Beispielsweise ist ein maximal zulässiger variabler Zusatznominalwertanteil für das Banknotenkonto der entsprechenden Banknote in einem von der Zentralbank verwalteten Register ein-

getragen. Beispielsweise beträgt der maximal zulässiger variabler Zusatznominalwertanteil der Banknote 100%, 200%, 300%, 400%, 500%, 600%, 700%, 800%, 900% oder 1000% des Mindestnominalwert der Banknote. Beispielsweise ist ein maximal zulässiger variable Zusatznominalwertanteil für alle von der Zentralbank ausgegebene Banknoten nach oben einheitlich begrenzt. Beispielsweise wird bei einer Transaktion an ein Banknotenkonto einer Banknote als Voraussetzung zum Ausführen der Transaktion geprüft, ob durch die Transaktion der maximal zulässige variable Zusatznominalwertanteil überschritten wird. Falls der maximal zulässige variable Zusatznominalwertanteil nicht überschritten wird, wird die Transaktion ausgeführt. Falls der maximal zulässige variable Zusatznominalwertanteil überschritten wird, wird die Transaktion nicht ausgeführt.

[0026] Die Banknote kann beispielsweise papier- und/oder kunststoffbasiert sein. Beispielsweise umfasst die Banknote ein oder mehrere Materialschichten. Als Materialien für die Materialschichten können beispielsweise Papier, Kunststoffe und/oder Metallfolien Verwendung finden. Ein Materialschicht kann auch Kombinationen mehreren dieser Materialen umfassen. Beispielsweise sind die Materialschichten zusammenlaminiert. Die Materialschichten können insbesondere elektronische Komponenten, etwa ein Sicherheitselement mit Prozessor und Speicher, eine Antenne, ein Display, eine Eingabevorrichtung und/oder Sensoren, umfassen oder in Kombination miteinander bilden. Die Banknote ist beispielsweise flexibel.

[0027] Die Banknote umfasst beispielsweise eine Mehrzahl von Sicherheitsmerkmale, welche es ermöglichen die Authentizität und Validität der Banknoten zu prüfen. Die Mehrzahl von Sicherheitsmerkmale kann beispielsweise ein oder mehrere Level 1, Level 2 und/oder Level 3 Sicherheitsmerkmale umfassen. Level 1 Sicherheitsmerkmale sind Sicherheitsmerkmale, welche vom Menschen direkt erkannt und ohne weitere Hilfsmittel überprüft werden können. Level 2 Sicherheitsmerkmale sind maschinenlesbare Sicherheitsmerkmale, welche beispielsweise für kommerzielle Anforderungen zur Echtheitsprüfung von Banknoten verwendet werden. Level 3 Sicherheitsmerkmale sind Sicherheitsmerkmale, welche nur der ausgebenden Zentralbank bekannt. Zentralbanken verwenden solche geheim gehaltenen maschinenlesbaren Sicherheitsmerkmale, um die Integrität des Bargeldkreislaufs sicherzustellen und zu garantieren, nur echte Banknoten wieder in den Umlauf zu geben. Ferner verwenden Zentralbanken solche Level 3 Sicherheitsmerkmale, um echte Banknoten gegebenenfalls aus dem Umlauf zu nehmen und kontrolliert zu vernichten, falls die Umlauffähigkeit der entsprechenden Banknoten, beispielsweise aufgrund von Verschmutzung und/oder Verschleiß, nicht mehr ausreicht.

[0028] Die Sicherheitsmerkmale können beispielsweise taktile, akustische oder sichtbare Merkmale umfassen. Beispielsweise werden zur Herstellung der Banknote Materialien, wie etwa Sicherheitspapieren, mit einem charakteristischen haptischen Eindruck und/oder einem charakteristischen Klang beim Reiben und/oder Knüllen verwendet. Beispielsweise werden haptisch erfassbare Prägungen in die Banknote eingebracht. Beispielsweise werden visuell erfassbare Sicherheitsmerkmale, wie etwa Wasserzeichen, Durchsichtfenster, Durchsichtsregister, Passerdruckelemente, Folienelemente, Guillochen, Irisdruckelemente, Anti-Kopier-Raster, Melierfasern, Mikro-Perforationen, Mikroschriften, optisch variable Druckfarben, Perlglanzstreifen, Sicherheitsfaden und/oder Sonderfarben verwendet. Beispielsweise werden Sicherheitselemente wie etwa Metamerie-Farbkombinationen, Fluoreszierende Farben, diffraktive optische Elemente und/oder Scrambled-Indicia-Mikrodruckmuster verwendet.

[0029] Beispielsweise werden maschinenlesbare Sicherheitselemente verwendet, wie etwa Infraroteigenschaften der Druckfarbe, phosphoreszierende Farben, magnetische Elemente, Elemente mit charakteristischer elektrischer Leitfähigkeit und/oder Kopierschutzelemente, wie etwa ein digitales Wasserzeichen und/oder standardisierte Muster, beispielsweise eine EURion-Konstellation oder Omron-Ringe.

[0030] Beispielsweise umfasst die Banknote ein oder mehrere Sicherheitsmerkmale, welche nur der ausgebenden Zentralbank bekannt und/oder von dieser prüfbar sind, d.h. Level 3 Sicherheitsmerkmale, wie etwa das M-Feature der EZB.

[0031] Sicherheitsmerkmale, insbesondere Level 1 und Level 2 Sicherheitsmerkmale, können den Vorteil haben, dass sie es den Beteiligten ermöglichen eine Banknote ohne viel Aufwand auf ihre Echtheit, d.h. Authentizität und Validität, hin zu prüfen. Dies ermöglicht eine Verwendung der Banknote für Barzahlungen, welche eine Übergabe der Banknote von einem Zahlungspflichtigen an einen Zahlungsempfänger umfassen.

[0032] Unter einer „Kommunikationsschnittstelle“ wird hier beispielsweise eine Schnittstelle verstanden, über die Daten empfangen und gesendet werden können, wobei die Kommunikationsschnittstelle kontaktbehaftet oder kontaktlos konfiguriert sein kann.

[0033] Eine Kommunikation kann beispielsweise über ein Netzwerk erfolgen. Unter einem „Netzwerk“ wird hier jedes Übertragungsmedium mit einer Anbindung zur Kommunikation verstanden, insbesondere eine lokale Verbindung oder ein lokales Netzwerk, insbesondere ein Local Area Network (LAN), ein privates Netzwerk, insbesondere ein Intranet, und ein

digitales privates Netzwerk (Virtual Private Network - VPN). Beispielsweise kann ein Computersystem eine Standardfunkschnittstelle zur Anbindung an ein WLAN aufweisen. Ferner kann es sich um ein öffentliches Netzwerk, wie beispielsweise das Internet handeln. Je nach Ausführungsform kann diese Verbindung auch über ein Mobilfunknetz hergestellt werden.

[0034] Eine kontaktlose Kommunikation mit der Banknote ist beispielsweise mittels Near Field Communication (NFC) möglich. Hierbei handelt es sich um eine auf der RFID-Technologie basierende Kommunikation zum kontaktlosen Austausch von Daten per elektromagnetischer Induktion mittels loser gekoppelter Spulen über kurze Strecken, von beispielsweise wenigen Zentimetern. NFC kann beispielsweise gemäß einer der Normen ISO 14443, 18092, 21481, ECMA 340, 352, 356, 362 bzw. ETSI TS **102 190** implementiert sein.

[0035] Die Kommunikationsschnittstelle der Banknote umfasst beispielsweise eine Antenne zur kontaktlosen Kommunikation. Die Antenne umfasst beispielsweise eine Induktionsspule. Die Induktionsspule kann ferner konfiguriert sein zur externen Energieversorgung der Banknote, beispielsweise mittels Energy Harvesting. Beispielsweise ist die Induktionsspule dazu konfiguriert, dass ein Terminal Energie in die Banknote einkoppelt.

[0036] Unter einem „Prozessor“ wird hier und im Folgenden eine Logikschaltung verstanden, die zur Ausführung von Programminstruktionen dient. Die Logikschaltung kann auf einem oder mehreren diskreten Bauelementen implementiert sein, insbesondere auf einem Chip. Ein Prozessor umfasst beispielsweise ein Rechenwerk, ein Steuerwerk, Register und Datenleitungen zur Kommunikation mit anderen Komponenten. Insbesondere wird unter einem „Prozessor“ ein Mikroprozessor oder ein Mikroprozessorsystem aus mehreren Prozessorkernen und/oder mehreren Mikroprozessoren verstanden.

[0037] Unter einem „Speicher“ wird hier insbesondere ein nichtflüchtiger Speicher verstanden. Unter einem „nichtflüchtigen Speicher“ wird hier beispielsweise ein elektronischer Speicher zur dauerhaften Speicherung von Daten verstanden. Ein nichtflüchtiger Speicher kann als nichtänderbarer Speicher konfiguriert sein, der auch als Read-Only Memory (ROM) bezeichnet wird, oder als änderbarer Speicher, der auch als Non-Volatile Memory (NVM) bezeichnet wird. Insbesondere kann es sich hierbei um ein EEPROM, beispielsweise ein Flash-EEPROM, kurz als Flash bezeichnet, handeln. Ein nichtflüchtiger Speicher zeichnet sich dadurch aus, dass die darauf gespeicherten Daten auch nach Abschalten der Energieversorgung erhalten bleiben.

[0038] Unter einem „geschützten Speicherbereich“ wird hier ein Bereich eines elektronischen Speichers verstanden, auf den ein Zugriff, das heißt ein Lesezugriff oder ein Schreibzugriff, nur über einen Prozessor des Sicherheitselements möglich ist. Beispielsweise ist auf den geschützten Speicherbereich kein externer Zugriff möglich, d.h. Daten können hierher weder von außen eingebracht werden, noch nach außen ausgegeben werden. Beispielsweise können Daten über den Prozessor nach außen aus den geschützten Speicherbereich ausgelesen werden. Beispielsweise können Daten über den Prozessor von außen in den geschützten Speicherbereich eingebracht werden. Nach Ausführungsformen ist der Zugriff von dem bzw. über den mit dem Speicher gekoppelten Prozessor nur dann möglich, wenn eine hierzu erforderliche Bedingung erfüllt ist. Hierbei kann es sich zum Beispiel um eine kryptografische Bedingung, insbesondere eine erfolgreiche Authentisierung und/oder eine erfolgreiche Berechtigungsprüfung, handeln. Eine solche Prüfung kann beispielsweise auf einer elektronischen Signatur mit einem Signaturschlüssel beruhen.

[0039] Asymmetrische Schlüsselpaare werden für eine Vielzahl von Kryptosystemen eingesetzt und spielen auch bei der Signatur elektronischer Dokumente eine wichtige Rolle. Ein asymmetrisches Schlüsselpaar besteht aus einem öffentlichen Schlüssel, welcher zur Ver- und/oder Entschlüsselung von Daten verwendet wird und an Dritte weitergegeben werden darf, sowie einem privaten Schlüssel, welcher zur Ver- und/oder Entschlüsselung von Daten verwendet wird und im Regelfall geheim gehalten werden muss. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln und digitale mit dem privaten Schlüssel erstellte Signaturen zu prüfen. Ein privater Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln oder digitale Signaturen zu erstellen. Eine mit einem privaten Schlüssel erstellte Signatur kann mit dem zugehörigen öffentlichen Schlüssel verifiziert werden.

[0040] Die Erstellung einer digitalen Signatur, im Folgenden auch lediglich als „Signatur“ bezeichnet, ist ein kryptographisches Verfahren, bei dem zu beliebigen Daten ein weiterer Datenwert, welcher als „Signatur“ bezeichnet wird, berechnet wird. Bei einer Signatur kann es sich zum Beispiel um eine mit einem privaten kryptographischen Schlüssel verschlüsselten Hashwert der Ausgangsdaten handeln.

[0041] Unter eine Sicherheitselement wird hier beispielsweise eine elektronische Komponente verstanden, welche einen Prozessor und einen Speicher umfasst, und auf welche nur bestimmte vordefinierte Zugriffe ermöglicht werden. Beispielsweise können nur bestimmte Datenwerte, welche etwa in bestimmten

Bereichen des Speichers abgelegt sind ausgelesen werden. Beispielsweise können in einem geschützten Speicherbereich abgelegt Datenwerte nicht ausgelesen werden. Beispielsweise ist zum Schreiben eines Datenwerts in den Speicher des Sicherheitselements eine digitale Signatur notwendig, deren Prüfschlüssel in dem Sicherheitselement hinterlegt ist. Beispielsweise besitz nur der Prozessor Schreibrechte zum Schreiben von Daten in einen geschützten Speicherbereich.

[0042] Das Sicherheitselement stellt ferner beispielsweise kryptographische Kernroutinen in Form von kryptographischen Programminstruktionen mit kryptographischen Algorithmen für Signaturerstellung und/oder -prüfung, Schlüsselgenerierung, und/oder Zufallszahlengenerierung bereit und kann ferner als sicherer Speicher für kryptographische Schlüssel dienen.

[0043] Beispielsweise sind zumindest Teile des Sicherheitselements signiert. Vor einer Nutzung des Sicherheitselements wird geprüft, ob die Signatur bzw. die Signaturen, valide sind. Wenn eine der Signaturen nicht valide ist, wird die Nutzung des Sicherheitselements beispielsweise gesperrt.

[0044] Beispielsweise weist das Sicherheitselement physikalisch beschränkten Zugriffsmöglichkeiten. Zudem kann das Sicherheitselement I zusätzliche Maßnahmen gegen Missbrauch aufweisen, insbesondere gegen unberechtigte Zugriffe auf Daten im Speicher des Sicherheitselement. Beispielsweise umfasst ein Sicherheitselement Sensoren zur Überwachung des Zustands des Sicherheitselements sowie von dessen Umgebung, um Abweichungen vom Normalbetrieb zu erkennen, welche auf Manipulationsversuche hinweisen können. Entsprechende Sensortypen umfassen beispielweise einen Taktfrequenzsensor, einen Spannungssensor und/oder einen Lichtsensor. Taktfrequenzsensoren und Spannungssensoren erfassen beispielweise Abweichungen der Taktfrequenz, Temperatur und/oder Spannung nach oben oder unten von einem vordefinierten Normalbereich. Insbesondere kann ein Sicherheitselement nichtflüchtige Speicher mit einem geschützten Speicherbereich umfassen.

[0045] Beispielsweise umfassen die Mittel zum Schutz des Sicherheitselements gegen unbefugte Manipulationen mechanische Mittel, die z.B. das Öffnen des Sicherheitselements oder seiner Teile verhindern sollen, oder die bei dem Versuch eines Eingriffs in das Sicherheitselement dieses unbrauchbar machen, beispielsweise indem ein Datenverlust eintritt. Beispielsweise können hierzu zumindest Teile des Sicherheitselements in ein Material eingeschlossen, eingegossen und/oder einlaminiert sein, dessen versuchte Entfernung zu einer unvermeidlichen Zerstörung der entsprechenden Teile des Sicherheitselements führt.

[0046] Bei den visuellen Angaben handelt es sich beispielsweise um Informationen, welche in einer optisch lesbaren Form in die Banknote eingebracht sind. Beispielsweise sind diese Informationen auf die Banknote und/oder eine Materialschicht der Banknote aufgedruckt, eingeprägt, eingraviert, aus dieser ausgestanzt, ausgeschnitten oder auf eine sonstige optisch erfassbare Weise eingebracht. Diese visuellen Merkmale sind beispielsweise mit einem optischen Sensor, wie etwa einer Kamera, erfassbar.

[0047] Das Kryptogramm resultiert aus der Anwendung eines kryptographischen Algorithmus. Dabei werden beispielsweise die Identifikationsnummer der Banknote und ein zahlungsindividueller Code als Eingangswerte mit dem banknotenindividuellen kryptographischen Schlüssel verschlüsselt.

[0048] Nach Ausführungsformen ist die Identifikationsnummer ebenfalls in dem geschützten Speicherbereich des Speichers des Sicherheitselements gespeichert. Ausführungsformen können den Vorteil haben, dass die Identifikationsnummer ebenfalls vor effizient vor unberechtigten Zugriffen geschützt werden kann.

[0049] Nach Ausführungsformen umfasst die Banknote eine Mehrzahl von Sicherheitsmerkmalen. Ausführungsformen können den Vorteil haben, dass es unter Verwendung der Sicherheitsmerkmale, bei welchen es sich beispielsweise um Level 1, Level 2 und/oder Level 3 Sicherheitsmerkmale handelt, ermöglicht werden kann die Authentizität und Validität der Banknote zu prüfen. Nach Ausführungsformen umfassen ein oder mehrere Sicherheitsmerkmale der Mehrzahl von Sicherheitsmerkmalen eine Angabe der Seriennummer und/oder der Identifikationsnummer der Banknote. Ausführungsformen können den Vorteil haben, dass bei einem Erfassen der entsprechenden ein oder mehreren Sicherheitsmerkmale jeweils die Seriennummer und/oder der Identifikationsnummer der Banknote miterfasst werden kann. Als Bestandteil der entsprechenden Sicherheitsmerkmale kann anhand der Sicherheitsmerkmale nicht nur die Authentizität und Validität der Banknote an sich, sondern auch die Authentizität und Validität der Seriennummer und/oder der Identifikationsnummer der Banknote geprüft werden. Somit kann beispielsweise eine durch die entsprechenden Sicherheitsmerkmale gesicherte Verbindung bzw. Zuordnung der physischen Banknote und dem Banknotenkonto der Banknote bereitgestellt werden, welches beispielsweise unter Verwendung der Seriennummer und/oder der Identifikationsnummer der Banknote identifizierbar ist. Nach Ausführungsformen handelt es sich bei den ein oder mehreren Sicherheitsmerkmalen, welche eine Angabe der Seriennummer und/oder der Identi-

fikationsnummer der Banknote umfassen, beispielsweise um Level 1, Level 2 und/oder Level 3 Sicherheitsmerkmale.

[0050] Nach Ausführungsformen umfasst die Banknote die visuelle Angabe der Seriennummer mehrfach über die Banknote verteilt. Ausführungsformen können den Vorteil haben, dass selbst bei einer teilweisen Beschädigung der Banknote, die Seriennummer erfasst werden kann. Beispielsweise sind Angaben der Seriennummer in Kombination mit und/oder als Bestandteil von mehreren Sicherheitsmerkmalen der Banknote in diese eingebracht. Dies könnte den Vorteil haben, dass solange genügend Sicherheitsmerkmale zur Bestätigung der Authentizität und Validität der Banknote vorliegen, die Seriennummer der Banknote erfasst werden kann.

[0051] Nach Ausführungsformen ist die Mehrzahl von Angaben der Seriennummer derart über die Banknote verteilt, dass sichergestellt werden kann, dass die Seriennummer der Banknote ermittelt werden kann, solange mehr als 50% der Banknote vorliegen. Ausführungsformen können den Vorteil haben, dass bei einem Verlust eines Teils der Banknote sichergestellt werden kann, dass solange mehr als 50% der Banknote vorliegen, was beispielsweise Voraussetzung für ein Ersetzen der Banknote ist, die vorliegenden mehr als 50% die Seriennummer der Banknote umfassen. Somit kann selbst bei einem teilweisen Verlust der Banknote sichergestellt, dass solange der verbliebene Teil bzw. die verbliebenen Teile der Banknote valide sind, die Seriennummer erfasst und der aktuelle Nominalwert der Banknote gemäß dem Banknotenkonto bestimmt werden kann.

[0052] Nach Ausführungsformen handelt es sich bei der Identifikationsnummer um eine Banknotenkontonummer des der Banknote individuell zugeordneten anonymen Banknotenkontos. Nach Ausführungsformen handelt es sich bei der Identifikationsnummer um eine unabhängig von der Seriennummer der Banknote erzeugte Nummer. Nach Ausführungsformen ist die unabhängig erzeugte Identifikationsnummer der Seriennummer der Banknote zugeordnet. Beispielsweise ist die Identifikationsnummer der Seriennummer unter Verwendung eines Eintrags in einem von der Zentralbank verwalteten Register zugeordnet, welcher die Identifikationsnummer der Seriennummer zuordnet.

[0053] Nach Ausführungsformen handelt es sich bei der Identifikationsnummer um die Seriennummer der Banknote. Nach Ausführungsformen handelt es sich bei der Identifikationsnummer um eine unter Verwendung der Seriennummer erzeugte Banknotenkontonummer des der Banknote individuell zugeordneten anonymen Banknotenkontos. Ausführungsformen können den Vorteil haben, dass anhand der von Angaben der Banknote, wie beispielsweise der Seriennummer der Banknote, das zugehörige Banknotenkonto identifiziert und somit der aktuelle Nominalwert der Banknote ermittelt werden kann.

[0054] Nach Ausführungsformen handelt es sich bei der Identifikationsnummer um eine Identifikationsnummer, welche der Banknotenkontonummer des der Banknote individuell zugeordneten anonymen Banknotenkontos, beispielsweise in einem Registereintrag eines von der ausgebenden Zentralbank verwalteten Registers, zugeordnet ist. Nach Ausführungsformen wird die Identifikationsnummer unabhängig von der Seriennummer der Banknote erzeugt und dieser, beispielsweise in einem Registereintrag eines von der ausgebenden Zentralbank verwalteten Registers, zugeordnet. Nach Ausführungsformen wird die Identifikationsnummer unabhängig von der Banknotenkontonummer des der Banknote individuell zugeordneten anonymen Banknotenkontos erzeugt und dieser, beispielsweise in einem Registereintrag eines von der ausgebenden Zentralbank verwalteten Registers, zugeordnet.

[0055] Ausführungsformen können den Vorteil haben, dass bei einer registerbasierten Zuordnung Zugriff auf das Register notwendig sein kann, um für eine Banknote das zugehörige Banknotenkonto ermitteln zu können. Bei einem von der ausgebenden Zentralbank verwalteten Register, ist es beispielsweise alleine der entsprechenden Zentralbank möglich das einer Banknote zugehörige Banknotenkonto zu ermitteln.

[0056] Nach Ausführungsformen umfasst der zahlungsindividuelle Code einen Zeitstempel
und/oder eine Zufallszahl. Ausführungsformen können den Vorteil haben, dass das Kryptogramm für jede Zahlung effizient individualisiert werden kann. Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann, dass Kryptogramm effizient individualisiert werden können. Mit anderen Worten kann so beispielsweise ausgeschlossen werden, dass für zwei verschiede Zahlungen mit derselben Banknote dasselbe Kryptogramm erzeugt wird, selbst bei Zahlung identischer Beträge an identische Zahlungsempfänger. Wird beispielsweise der Zentralbank ein Kryptogramm zur Autorisierung einer Zahlung vorgelegt, welches von der Zentralbank bereits verarbeitet wurde, folgt daraus, dass das vorgelegte Kryptogramm nicht(mehr) gültig ist.

[0057] Nach Ausführungsformen handelt es sich bei dem banknotenindividuellen kryptographischen Schlüssel um einen symmetrischen kryptographischen Schlüssel. Nach Ausführungsformen handelt es sich bei dem banknotenindividuellen kryptographischen Schlüssel um einen privaten kryptographischen Schlüssel eines banknotenindividuellen asymmetrischen Schlüsselpaars.

[0058] Nach Ausführungsformen handelt es sich bei der Seriennummer und/oder bei der Identifikationsnummer der Banknote um den einen öffentlichen kryptographischen Schlüssel des banknotenindividuellen asymmetrischen Schlüsselpaars der Banknote, um einen aus dem öffentlichen kryptographischen Schlüssel der Banknote abgeleitete Nummer und/der eine dem öffentlichen kryptographischen Schlüssel der Banknote zugeordneten Nummer. Eine entsprechende Zuordnung kann beispielsweise unter Verwendung eines entsprechenden Zuordnungseintrags in einem von der ausgebenden Zentralbank verwalteten Registers erfolgen.

[0059] Nach Ausführungsformen umfasst die Banknote eine visuelle Angabe des öffentlichen kryptographischen Schlüssels der Banknote, eines aus dem öffentlichen kryptographischen Schlüssel der Banknote abgeleiteten Werts und/oder eines dem öffentlichen kryptographischen Schlüssel der Banknote zugeordneten Werts. Eine entsprechende Zuordnung kann beispielsweise unter Verwendung eines entsprechenden Zuordnungseintrags in einem von der ausgebenden Zentralbank verwalteten Registers erfolgen.

[0060] Nach Ausführungsformen umfassen ein oder mehrere Sicherheitsmerkmale der Mehrzahl von Sicherheitsmerkmalen eine Angabe des öffentlichen kryptographischen Schlüssels der Banknote, eines aus dem öffentlichen kryptographischen Schlüssel der Banknote abgeleiteten Werts und/oder eines dem öffentlichen kryptographischen Schlüssel der Banknote zugeordneten Werts. Eine entsprechende Zuordnung kann beispielsweise unter Verwendung eines entsprechenden Zuordnungseintrags in einem von der ausgebenden Zentralbank verwalteten Registers erfolgen. Ausführungsformen können den Vorteil haben, dass bei einem Erfassen der entsprechenden ein oder mehreren Sicherheitsmerkmale jeweils der öffentliche kryptographische Schlüssels der Banknote, ein aus dem öffentlichen kryptographischen Schlüssel der Banknote abgeleiteter Wert und/oder ein dem öffentlichen kryptographischen Schlüssel der Banknote zugeordneter Wert miterfasst werden kann. Als Bestandteil der entsprechenden Sicherheitsmerkmale kann anhand der Sicherheitsmerkmale nicht nur die Authentizität und Validität der Banknote an sich, sondern auch die Authentizität und Validität des öffentlichen kryptographischen Schlüssels der Banknote, eines aus dem öffentlichen kryptographischen Schlüssel der Banknote abgeleiteten Werts und/oder eines dem öffentlichen kryptographischen Schlüssel der Banknote zugeordneten Werts geprüft werden. Somit kann beispielsweise eine durch die entsprechenden Sicherheitsmerkmale gesicherte Verbindung bzw. Zuordnung der physischen Banknote und dem Banknotenkonto der Banknote bereitgestellt werden, welches beispielsweise unter Verwendung des öffentlichen kryptographischen Schlüssels der Banknote, eines aus dem öffentlichen kryptographischen Schlüssel der Banknote abgeleiteten Werts und/oder eines dem öffentlichen kryptographischen Schlüssel der Banknote zugeordneten Werts identifizierbar ist. Nach Ausführungsformen handelt es sich bei den ein oder mehreren Sicherheitsmerkmalen, welche eine Angabe der Seriennummer und/oder der Identifikationsnummer der Banknote umfassen, beispielsweise um Level 1, Level 2 und/oder Level 3 Sicherheitsmerkmale.

[0061] Nach Ausführungsformen gibt die Zahlungsanfrage einen zu zahlenden Betrag an und der zu zahlende Betrag wird als zusätzlicher Eingangswert zum Erzeugen des zahlungsindividuellen Kryptogramms verwendet. Ausführungsformen können den Vorteil haben, dass bei der Individualisierung des Kryptogramms ferner der zu zahlenden Betrag berücksichtigt wird.

[0062] Nach Ausführungsformen umfasst die Zahlungsautorisierung ferner die Identifikationsnummer und/oder den zahlungsindividuellen Code in Klartext. Ausführungsformen können den Vorteil haben, dass die in Klartext bereitgestellte Identifikationsnummer und/oder der zahlungsindividuelle Code zur Prüfung der Validität des Kryptogramms verwendet werden können. Ferner kann unter Verwendung der Identifikationsnummer das Banknotenkonto identifiziert werden, von welchem die Zahlung erfolgen soll.

[0063] Nach Ausführungsformen umfasst die Zahlungsautorisierung ferner den zu zahlenden Betrag in Klartext. Ausführungsformen können den Vorteil haben, dass der in Klartext bereitgestellte Betrag zur Prüfung der Validität des Kryptogramms verwendet werden können. Ferner ist so der zu zahlende Betrag ohne zusätzliche kryptographische Verarbeitungsschritte ersichtlich.

[0064] Nach Ausführungsformen umfasst die Banknote eine Kommunikationsschnittstelle zur Kommunikation mit einem Terminal. Die Banknote empfängt die Zahlungsanfrage von dem Terminal über die Kommunikationsschnittstelle und/oder sendet die Zahlungsautorisierung über die Kommunikationsschnittstelle an das Terminal.

[0065] Nach Ausführungsformen umfasst die Banknote eine Nutzerschnittstelle zur Kommunikation mit einem Nutzer der Banknote, wobei die Banknote die Zahlungsanfrage von einem Nutzer über eine Eingabevorrichtung der Nutzerschnittstelle empfängt und/oder die Zahlungsautorisierung an die Nutzerschnittstelle zum Ausgeben über eine Anzeigevorrichtung der Nutzerschnittstelle sendet. Bei dem Terminal kann es sich beispielsweise um ein Terminal eines Verkäufers an einem Verkaufsort (engl.: „Point of Sale“/PoS), d.h. an dem Ort, an dem ein Verkauf voll-

zogen wird, handeln. Bei dem Terminal kann es sich ferner um ein Terminal handeln, welches an ein Nutzercomputersystem angeschlossen ist, über welches eine Zahlung mit der Banknote abgewickelt werden soll. Beispielsweise handelt es sich hierbei um eine Zahlungsabwicklung über ein Netzwerk, etwa das Internet, gegenüber einem Dienstanbieter, sei es ein Verkäufer oder ein Zahlungsdienstanbieter. Ebenso könnte das Terminal in Form eines mobilen tragbaren Kommunikationsgeräts, etwa einem Smartphone, eines Nutzers bereitgestellt werden. Der Nutzer könnte das mobile tragbare Kommunikationsgerät beispielsweise für eine Zahlungsabwicklung über ein Netzwerk, etwa das Internet, gegenüber einem Dienstanbieter nutzen, sei es ein Verkäufer oder ein Zahlungsdienstanbieter.

[0066] Nach Ausführungsformen umfasst die Banknote eine Nutzerschnittstelle zur Kommunikation mit einem Nutzer der Banknote, wobei die Banknote die Zahlungsanfrage von einem Nutzer über eine Eingabevorrichtung der Nutzerschnittstelle empfängt und/oder die Zahlungsautorisierung an die Nutzerschnittstelle zum Ausgeben über eine Anzeigevorrichtung der Nutzerschnittstelle sendet. Ausführungsformen können den Vorteil haben, dass die für den Nutzer sichtbar ist und/oder gesteuert wird, welche Daten in die Banknote eingegeben werden und welche Daten die Banknote ausgibt.

[0067] Die Eingabevorrichtung kann beispielsweise ein Touch-Pad umfassen. Die Anzeigevorrichtung kann beispielsweise ein Display umfassen. Die Eingabevorrichtung kann beispielsweise mit der Anzeigevorrichtung kombiniert sein, etwa in Form eines Touch-Displays. Der Nutzer gibt die Daten der Zahlungsanfrage beispielsweise unter Verwendung der Eingabevorrichtung in Banknote ein.

[0068] Beispielsweise wird dem Nutzer die Zahlungsanfrage und/oder die Zahlungsautorisierung auf der Anzeigevorrichtung der Banknote angezeigt. Eine Bestätigung der angezeigten Zahlungsanfrage und/oder Zahlungsautorisierung durch den Nutzer unter Verwendung der Eingabevorrichtung der Banknote ist beispielsweise Voraussetzung für ein Erzeugen der Zahlungsautorisierung.

[0069] Beispielsweise wird die Zahlungsautorisierung an die Anzeigevorrichtung der Banknote zum Anzeigen gesendet, etwa als alphanumerischer Zeichenfolg, Bar-Code, oder QR-Code. Die auf der Anzeigevorrichtung angezeigte Zahlungsautorisierung kann beispielsweise unter Verwendung eines optischen Sensors, etwa eines Sensors eines Terminals, gescannt bzw. eingelesen werden.

[0070] Nach Ausführungsformen ist in dem Speicher des Sicherheitselements ferner ein aktueller Nominalwert der Banknote gespeichert. Ausführungsformen können den Vorteil haben, dass der aktuelle Nominalwert aus der Banknote ausgelesen werden kann. Beispielsweise legt den tatsächlich verbindlichen Nominalwert der Banknote aber der Kontostand des zugehörigen Banknotenkontos fest.

[0071] Beispielsweise ist der aktuelle Nominalwert in dem geschützten Speicherbereich des Speichers des Sicherheitselements gespeichert. Beispielsweise ist der aktuelle Nominalwert nicht in dem geschützten Speicherbereich des Speichers des Sicherheitselements gespeichert. Beispielsweise ist der in dem Speicher des Sicherheitselements gespeicherte aktueller Nominalwert der Banknote von außen auslesbar. Beispielsweise ist der in dem Speicher des Sicherheitselements gespeicherte aktueller Nominalwert der Banknote nicht von außen auslesbar. Beispielsweise dient der in dem Speicher des Sicherheitselements gespeicherte aktueller Nominalwert der Banknote alleine einer internen Prüfung, etwa, ob ein zu zahlender Betrag kleiner gleich dem aktuellen Nominalwert der Banknote ist.

[0072] Nach Ausführungsformen ist ferner die Seriennummer der Banknote in dem Speicher des Sicherheitselements gespeichert.

[0073] Nach Ausführungsformen ist initial als aktueller Nominalwert der initiale Nominalwert der Banknote in dem Speicher des Sicherheitselements gespeichert. Ausführungsformen können den Vorteil haben, dass ausgehend von diesem initialen Nominalwert bei jeder erfolgreich abgewickelten Zahlung der gespeicherte Nominalwert angepasst wird und somit banknotenseitig der aktuelle Nominalwert nachverfolgt werden kann.

[0074] Nach Ausführungsformen ist der Prozessor ferner dazu konfiguriert bei Ausführen der Programminstruktionen den zu zahlenden Betrag mit dem gespeicherten aktuellen Nominalwert der Banknote abzugleichen und das zahlungsindividuelle Kryptogramms zur Autorisierung der Zahlung nur unter der Voraussetzung zu erzeugen, dass der gespeicherte aktuelle Nominalwert größer oder gleich dem zu zahlenden Betrag ist. Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann, dass der aktuelle Nominalwert für die auszuführende Zahlung ausreichend ist.

[0075] Nach Ausführungsformen ist der Prozessor ferner dazu konfiguriert bei Ausführen der Programminstruktionen ein Aktualisierungsverfahren zum Aktualisieren des gespeicherten aktuellen Nominalwerts der Banknote auszuführen. Das Aktualisierungsverfahren umfasst:

- Empfangen einer Aktualisierungsanfrage zum Aktualisieren des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote, wobei die Aktualisierungs-

anfrage einen aktualisierten Nominalwert der Banknote zusammen mit einer kryptographisch gesicherten Bestätigung der ausgebenden Zentralbank für den aktualisierten Nominalwert umfasst,

• Prüfen der kryptographisch gesicherten Bestätigung unter Verwendung eines in dem Speicher des Sicherheitselements gespeicherten kryptographischen Prüfschlüssels,

• im Falle einer erfolgreichen Prüfung, Ersetzten des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote mit dem empfangenen aktualisierten Nominalwert.

[0076] Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann der gespeicherte Nominalwert aktualisiert ist. Nach Ausführungsformen handelt es sich bei dem kryptographischen Prüfschlüssel um den banknotenindividuellen kryptographischen Schlüssel, beispielsweise um einen symmetrischen kryptographischen Schlüssel. Nach Ausführungsformen handelt es sich bei dem kryptographischen Prüfschlüssel um einen zusätzlichen zu dem banknotenindividuellen kryptographischen Schlüssel in dem Speicher des Sicherheitselements gespeicherten kryptographischen Prüfschlüssel, beispielsweise einen öffentlichen kryptographischen Schlüssel eines der Zentralbank zugeordneten asymmetrischen Schlüsselpaars. Der Signaturprüfschlüssel wird beispielsweise im Zuge der Herstellung der Banknote in dem Sicherheitselement hinterlegt.

[0077] Nach Ausführungsformen wird die Aktualisierungsanfrage in Antwort auf das Senden der Zahlungsautorisierung empfangen. Beispielsweise handelt es sich bei der Bestätigung der Zentralbank für den aktualisierten Nominalwert um eine Zahlungsbestätigung der Zentralbank. Beispielsweise handelt es sich bei dem aktualisierten Nominalwert um den bisherigen Nominalwert der Banknote abzüglich des gezahlten Betrags.

[0078] Nach Ausführungsformen wird die Aktualisierungsanfrage in Antwort auf einen Zahlungstransfer eines zusätzlichen Betrags auf das der Banknote individuell zugeordnete anonyme Banknotenkonto gesendet. Beispielsweise handelt es sich bei dem aktualisierten Nominalwert um den bisherigen Nominalwert der Banknote zuzüglich des zusätzlichen Betrags. Ausführungsformen können den Vorteil haben, dass auch Änderungen des Nominalwerts im Zuge eines Zahlungstransfer eines zusätzlichen Betrags auf das der Banknote berücksichtigt werden.

[0079] Nach Ausführungsformen ist für einen Zahlungstransfer eines zusätzlichen Betrags auf das Banknotenkonto der Banknote keine Autorisierung durch die entsprechende Banknote notwendig.

[0080] Nach Ausführungsformen ist für einen Zahlungstransfer eines zusätzlichen Betrags auf das Banknotenkonto der Banknote eine Autorisierung durch die entsprechende Banknote notwendig. Die Autorisierung erfolgt beispielweise analog zu der Autorisierung von Zahlungen mit der Banknote. Die Autorisierung umfasst beispielsweise:

• Empfangen einer Zahlungsanfrage für eine Zahlung auf das Banknotenkonto der Banknote,

• Erzeugen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung auf das Banknotenkonto der Banknote, wobei das Kryptogramm aus der Identifikationsnummer der Banknote und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt wird,

• Senden einer das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung.

[0081] Das zahlungsindividuelle Kryptogramm zur Autorisierung der Zahlungstransfers des zusätzlichen Betrags auf das Banknotenkonto der Banknote kann beispielsweise in analoger Weise zu dem zahlungsindividuellen Kryptogramm zur Autorisierung von Zahlungen mit der Banknote gebildet werden. Ausführungsformen können den Vorteil haben, dass sichergestellt erden kann, dass die Banknote Kenntnis von Zahlungen auf das Banknotenkonto und damit verbunden Änderungen des Nominalwerts der Banknote erhält.

[0082] Nach Ausführungsformen umfasst die kryptographisch gesicherte Bestätigung der ausgebenden Zentralbank den verschlüsselten aktualisierten Nominalwert der Banknote. Nach Ausführungsformen umfasst die kryptographisch gesicherte Bestätigung der ausgebenden Zentralbank den aktualisierten Nominalwert zusammen mit der Identifikationsnummer und/oder der Seriennummer der Banknote in verschlüsselter Form. Nach Ausführungsformen umfasst die kryptographisch gesicherte Bestätigung der ausgebenden Zentralbank den aktualisierten Nominalwert zusammen mit einem Zeitstempel in verschlüsselter Form. Nach Ausführungsformen wird zunächst eine Hashfunktion auf die zu verschlüsselnden Daten, beispielsweise aktualisierter Nominalwert, Identifikationsnummer, Seriennummer und/oder Zeitstempel, angewendet und der resultierende Hashwert verschlüsselt.

[0083] Nach Ausführungsformen wird die kryptographisch gesicherte Bestätigung ferner zusammen mit der Banknotenkontonummer, der Seriennummer der Banknote und/oder dem Zeitstempel empfangen. Nach Ausführungsformen umfasst die Aktuali-

sierungsanfrage neben dem aktualisierten Nominalwert die Identifikationsnummer der Banknote, die Seriennummer der Banknote und/oder den Zeitstempel in Klartext. Nach Ausführungsformen wird die kryptographisch gesicherte Bestätigung zum Prüfen unter Verwendung des Prüfschlüssels entschlüsselt und ein der Hashwert mit einem, beispielsweise unter Verwendung der mitgesendeten Klartextdaten, berechneten Referenzhashwert verglichen. Bei einer Übereinstimmung ist die Prüfung erfolgreich.

[0084] Nach Ausführungsformen ist der aktualisierte Nominalwert unter Verwendung des banknotenindividuellen kryptographischen Schlüssels in Form eines symmetrischen kryptographischen Schlüssels verschlüsselt. Nach Ausführungsformen handelt es sich bei dem Prüfschlüssel um den banknotenindividuellen kryptographischen Schlüssel in Form eines symmetrischen kryptographischen Schlüssels, unter dessen Verwendung die kryptographisch gesicherte Bestätigung zum Prüfen entschlüsselt werden kann.

[0085] Nach Ausführungsformen ist der aktualisierte Nominalwert unter Verwendung des eines privaten kryptographischen Schlüssels eines der Zentralbank zugeordneten asymmetrischen Schlüsselpaars verschlüsselt, welcher als Signaturschlüssel dient. Nach Ausführungsformen handelt es sich bei dem Prüfschlüssel um einen in dem Speicher des Sicherheitselements gespeicherten öffentlichen kryptographischen Schlüssel des der Zentralbank zugeordneten asymmetrischen Schlüsselpaars, unter dessen Verwendung die kryptographisch gesicherte Bestätigung zum Prüfen entschlüsselt werden kann.

[0086] Nach Ausführungsformen empfängt die Banknote die Aktualisierungsanfrage von einem Terminal über die Kommunikationsschnittstelle und/oder sendet den in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwert der Banknote über die Kommunikationsschnittstelle an das Terminal. Ausführungsformen können den Vorteil haben, dass das Terminal eine Kommunikationsverbindung für die Banknote zu der Zentralbank bzw. einem Server der Zentralbank bereitstellen kann.

[0087] Nach Ausführungsformen ist der Prozessor ferner dazu konfiguriert bei Ausführen der Programminstruktionen ein Ausgabeverfahren zum Ausgeben des gespeicherten aktuellen Nominalwerts der Banknote auszuführen. Das Ausgabeverfahren umfasst:

- Empfangen einer Ausgabeanfrage zum Ausgeben des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote,
- in Antwort auf die Ausgabeanfrage, Senden des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote.

[0088] Ausführungsformen können den Vorteil haben, dass der in der Banknote gespeicherte aktuelle Nominalwert direkt abgefragt werden kann und somit Kenntnis über diesen erhalten werden kann. Die Abfrage kann beispielsweise unter Verwendung eines Terminals oder, falls vorhanden, unter Verwendung einer Nutzerschnittstelle der Banknote erfolgen. Die Antwort wird beispielsweise an das Terminal oder an eine Anzeigevorrichtung der Nutzerschnittstelle zum Anzeigen gesendet.

[0089] Nach Ausführungsformen ist der gesendete aktuelle Nominalwerts der Banknote mit dem banknotenindividuellen kryptographischen Schlüssel in Form eines privaten kryptographischen Schlüssels eines der Banknote zugeordneten asymmetrischen Schlüsselpaars signiert. Nach Ausführungsformen kann der Empfänger des signierten aktuelle Nominalwerts, beispielsweise ein Terminal wie etwa ein Terminal eines PoS, ein Nutzercomputersystem und/oder mobilen tragbaren Telekommunikationsgerät, die Signatur mit einem öffentlichen kryptographischen Schlüssel des der Banknote zugeordneten asymmetrischen Schlüsselpaars als Signaturprüfschlüssel prüfen.

[0090] Nach Ausführungsformen ist der gesendete aktuelle Nominalwert unsigniert. Beispielsweise wird eine Bestätigungsanfrage zum Bestätigen des empfangenen aktuellen Nominalwerts der Banknote an die Zentralbank gesendet.

[0091] Nach Ausführungsformen wird zusammen mit dem gespeicherten aktuellen Nominalwert der Banknote die Seriennummer und/oder die Identifikationsnummer der Banknote gesendet und dient dem Empfänger des aktuellen Nominalwerts als Identifikator der Banknote für eine Bestätigungsanfrage an die Zentralbank zum Bestätigen des empfangenen aktuellen Nominalwerts der Banknote.

[0092] Nach Ausführungsformen umfasst die Banknote eine Kommunikationsschnittstelle zur kontaktlosen Kommunikation mit einem mobilen tragbaren Telekommunikationsgerät. Die Banknote empfängt die Ausgabeanfrage von dem mobilen tragbaren Telekommunikationsgerät über die Kommunikationsschnittstelle und/oder sendet den in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote über die Kommunikationsschnittstelle an das mobile tragbare Telekommunikationsgerät.

[0093] Nach Ausführungsformen umfasst die Banknote eine Nutzerschnittstelle zur Kommunikation mit einem Nutzer der Banknote. Die Banknote empfängt die Ausgabeanfrage von einem Nutzer über eine Eingabevorrichtung der Nutzerschnittstelle und/oder sendet den in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote

an die Nutzerschnittstelle zum Ausgeben über eine Anzeigevorrichtung der Nutzerschnittstelle.

[0094] Nach Ausführungsformen ist der Prozessor ferner dazu konfiguriert bei Ausführen der Programminstruktionen ein Ausgabeverfahren zum Ausgeben der in dem Speicher des Sicherheitselements gespeicherten Identifikationsnummer und/oder Seriennummer der Banknote auszuführen, wobei das Ausgabeverfahren umfasst:

- Empfangen einer Ausgabeanfrage zum Ausgeben der in dem Speicher des Sicherheitselements gespeicherten Identifikationsnummer und/oder Seriennummer der Banknote,
- in Antwort auf die Anfrage, Senden der in dem Speicher des Sicherheitselements gespeicherten Identifikationsnummer und/oder Seriennummer der Banknote.

[0095] Nach Ausführungsformen dient die Seriennummer und/oder die Identifikationsnummer der Banknote dem Empfänger als Identifikator der Banknote für eine Abfrage des aktuellen Nominalwerts der Banknote bei der ausgebenden Zentralbank. Ausführungsformen können den Vorteil haben, dass mit einem entsprechenden Identifikator die aktuellen Nominalwerte der Banknote bei der ausgebenden Zentralbank abgefragt und mithin in zuverlässiger Form Kenntnis von diesem erlangt werden kann.

[0096] Ausführungsformen umfassen ein Verfahren zum Ausstellen einer Banknote. Das Ausstellverfahren umfasst:

- Herstellen der Banknote, wobei die Banknote ferner ein Sicherheitselement mit einem Prozessor und einem Speicher mit Programminstruktionen umfasst,
- Empfang einer Identifikationsnummer der Banknote über einen ersten kryptographisch gesicherten Kanal, wobei die Identifikationsnummer ein von einer die Banknote ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote individuell zugeordnetes anonymes Banknotenkonto identifiziert,
- Speichern der empfangenen Identifikationsnummer in dem Speicher des Sicherheitselements,
- Empfang eines banknotenindividuellen kryptographischen Schlüssels über einen von dem ersten Kanal unabhängigen zweiten kryptographisch gesicherten Kanal,
- Speichern des empfangenen banknotenindividuellen kryptographischen Schlüssels in einem geschützten Speicherbereich des Speichers des Sicherheitselements.

[0097] Nach Ausführungsformen umfasst die hergestellte Banknote beispielsweise eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer der Banknote aus einem vordefinierten Bereich von Seriennummern. Nach Ausführungsformen umfasst die hergestellte Banknote beispielsweise eine visuelle Angabe der Identifikationsnummer. Nach Ausführungsformen umfasst die hergestellte Banknote beispielsweise eine visuelle Angabe eines der Banknote zugeordneten initialen Nominalwerts.

[0098] Ausführungsformen können den Vorteil haben, dass die Banknote in sicherer Weise initialisiert werden kann, d.h. Identifikationsnummer und banknotenindividuellen kryptographischen Schlüssel eingebracht werden können.

[0099] Nach Ausführungsformen ist das Ausstellverfahren dazu konfiguriert jede der zuvor beschriebenen Ausführungsformen der Banknote auszustellen. Nach Ausführungsformen handelt es sich bei der unter Verwendung des Ausstellverfahrens ausgestellten Banknote um eine Banknote nach einer der zuvor beschriebenen Ausführungsformen.

[0100] Nach Ausführungsformen wird die Identifikationsnummer ebenfalls in dem geschützten Speicherbereich des Speichers des Sicherheitselements gespeichert. Ausführungsformen können den Vorteil haben, dass die Identifikationsnummer sicher gespeichert werden kann.

[0101] Nach Ausführungsformen umfasst das Verfahren ferner ein Speichern des initialen Nominalwerts der Banknote als aktuellen Nominalwert in dem Speicher des Sicherheitselements. Nach Ausführungsformen umfasst das Verfahren ferner ein Speichern der Seriennummer der Banknote in dem Speicher des Sicherheitselements. Ausführungsformen können den Vorteil haben, dass der aktuelle Nominalwert und/oder die Seriennummer der Banknote von dieser in elektronsicher Form umfasst werden.

[0102] Nach Ausführungsformen umfasst das Verfahren ferner ein Speichern eines öffentlichen kryptographischen Schlüssels eines asymmetrischen Schlüsselpaars der ausgebenden Zentralbank. Nach Ausführungsformen wird der öffentlichen kryptographischen Schlüssel als Prüfschlüssel zum Prüfen von Signaturen der ausgebenden Zentralbank verwendet.

[0103] Nach Ausführungsformen umfasst das Verfahren ferner ein Senden einer Herstellungsbestätigung zu Bestätigung der Herstellung der Banknote an die ausgebende Zentralbank. Die Herstellungsbestätigung umfasst die Seriennummer und den initialen Nominalwert der hergestellten Banknote zum Speichern in einem ersten Register der ausgebenden Zentralbank. Der initiale Nominalwert gibt den

aktuellen Nominalwert der Banknote bei der Ausstellung an. Die Identifikationsnummer der Banknote und der banknotenindividuelle kryptographische Schlüssel werden in Antwort auf das Senden der Herstellungsbestätigung zum Speichern in dem Sicherheitselement empfangen.

[0104] Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann, dass die Herstellung der Banknote einhergeht mit einer zentralbankseitigen Initialisierung eines Banknotenkontos, welches der Banknote zugeordnet wird. Die Zuordnung erfolgt zentralbankseitig unter Verwendung der Seriennummer und des initialen Nominalwerts. Ferner werden die entsprechend zugeordnete Identifikationsnummer und der entsprechend zugeordnete banknotenindividuelle kryptographische Schlüssel der hergestellten Banknote zur Verfügung gestellt und die Zuordnung auch Banknotenseitig abzubilden.

[0105] Nach Ausführungsformen handelt es sich bei dem ersten Register um ein öffentlich zugängliches Register der Zentralbank. Nach Ausführungsformen dient die Seriennummer als ein Datenbankzugriffsschlüssel zum Auslesen des aktuellen Nominalwerts der Banknote aus dem ersten Register. Ausführungsformen können den Vorteil haben, dass der aktuelle Nominalwert einer Banknote allgemein zugänglich.

[0106] Nach Ausführungsformen werden die Identifikationsnummer und der banknotenindividuelle kryptographische Schlüssel in Antwort auf das Senden der Herstellungsbestätigung empfangen, nachdem die ausgebende Zentralbank die Identifikationsnummer und/oder den banknotenindividuellen kryptographischen Schlüssel in einem zweiten Register gespeicherte hat, welches die Identifikationsnummer und/oder den banknotenindividuellen kryptographischen Schlüssel der Seriennummer der Banknote zuordnet. Ausführungsformen können den Vorteil haben, dass die Verknüpfung bzw. Zuordnung zwischen physischer Banknote einerseits und digitalem Banknotenkonto andererseits durch eine entsprechende Eintragung in dem zweiten Register erfolgen kann.

[0107] Nach Ausführungsformen dient die Identifikationsnummer als ein Datenbankzugriffsschlüssel zum Auslesen der Seriennummer der Banknote und/oder des banknotenindividuellen kryptographischen Schlüssels aus dem zweiten Register. Nach Ausführungsformen dient die Seriennummer als ein Datenbankzugriffsschlüssel zum Auslesen der Identifikationsnummer der Banknote und/oder des banknotenindividuellen kryptographischen Schlüssels aus dem zweiten Register.

[0108] Nach Ausführungsformen sind die von der Zentralbank verwalteten Register, z.B. das erste und/oder das zweite Register als Blockchain implementiert. Nach Ausführungsformen handelt es sich bei der Identifikationsnummer der Banknote um eine Blockchainadresse der Banknote. Beispielswiese ist das Banknotenkonto unter Verwendung einer Blockchain bzw. als Blockchainadresse implementiert. Beispielsweise handelt es sich bei dem bei dem banknotenindividuellen kryptographischen Schlüssel um einen privaten kryptographischen Schlüssel eines banknotenindividuellen asymmetrischen Schlüsselpaars, welches ferner einen öffentlichen kryptographischen Schlüssel der Banknote umfasst, aus dem beispielsweise die Blockchainadresse der Banknote abgeleitet ist.

[0109] Unter einer „Blockchain“ wird hier und im Folgenden eine geordnete Datenstruktur verstanden, welche eine Mehrzahl von miteinander verketteten Datenblöcken umfasst. Insbesondere wird unter einer Blockchain eine geordnete Datenstruktur verstanden, bei welcher jeder der Blöcke (außer dem ersten Block) einen Prüfwert, beispielsweise einen Hash-Wert, seines Vorgängerblocks umfasst und somit anhand jedes Blocks die Gültigkeit aller seiner Vorgängerblocks geprüft und ggf. bestätigt werden kann. Für Beispiele einer Blockchain vergleiche https://en.wikipedia.org/wiki/Block_chain_(database) und „Mastering Bitcoin“, Chapter 7, The Blockchain, Seite **161** ff. Das Konzept der Blockchain wurde beispielsweise im Jahre 2008 in einem White Paper unter dem Pseudonym Satoshi Nakamoto zu Bitcoin beschrieben („Bitcoin: Peer-to-Peer Electronic Cash System“ (https://bitcoin.org/bitcoin.pdf)). Die darin beschriebene Blockchain besteht aus einer Reihe von Datenblöcken, in denen jeweils ein oder mehrere Einträge bzw. Transaktionen zusammengefasst und mit einer Prüfsumme in Form eines Hashwerts versehen sind. Zusätzliche Blöcke der Blockchain werden beispielsweise in einem rechenintensiven Prozess erzeugt, der auch als sogenanntes Mining bezeichnet wird. Diese zusätzlich erzeugten Blöcke werden anschließend der Blockchain hinzugefügt und über ein Netzwerk an alle Teilnehmer, bzw. Knoten des Netzwerks, verbreitet.

[0110] Ausführungsformen können den Vorteil haben, dass die Blockchain durch die Speicherung kryptografischer Prüfsumme, d.h. Hashwerten, des vorangehenden Blocks im jeweils nachfolgenden Block ein hohes Maß an Sicherheit gegenüber nachträglichen Manipulationen bietet. Das Verketten der Blöcke kann dann unter Verwendung dieser Root-Hashwerte überprüft werden. Jeder Block der Blockchain enthält in seinem Header den Hash des gesamten vorherigen Blockheaders. Somit wird die Reihenfolge der Blöcke eindeutig festgelegt und es entsteht eine Kettenstruktur. Durch die so implementierte Verkettung der einzelnen Blöcke miteinander wird erreicht, dass ein nachträgliches Modifizieren vorangegangener Blöcke bzw. einzelner Einträge praktisch ausgeschlossen ist, da hierfür die Hashwerte aller

nachfolgenden Blöcke in kurzer Zeit ebenfalls neu berechnet werden müssten.

[0111] Eine Blockchain kann beispielsweise auch in Form einer Blockchain implementiert werden, wobei nur eine ausgewählte Gruppe von Teilnehmern eine Berechtigung zum Hinzufügen gültiger Blöcke besitzt. Eine entsprechende Berechtigung kann beispielsweise mittels einer Signatur unter Verwendung eines privaten kryptographischen Schlüssels nachgewiesen werden. Der private kryptographische Schlüssel kann zu einem asymmetrischen Schlüsselpaar gehören, zu welchem auch ein öffentlicher kryptographischer Schlüssel gehört, mit dem die Signatur geprüft werden kann. Dem asymmetrischen Schlüsselpaar kann zudem beispielsweise ein Zertifikat zugeordnet sein, welches die Berechtigung zum Erzeugen eines gültigen Blocks der Blockchain belegt. Dieses Zertifikat kann ferner einer PKI zugeordnet sein, welche die Authentizität des Zertifikats belegt. Nach einer weiteren Ausführungsform kann beispielsweise für weitere Teilnehmer, welche der ausgewählten Gruppe hinzugefügt werden sollen, ein öffentlicher Schlüssel in der Blockchain in einem Initialisierungseintrag hinterlegt werden. Anhand dieser öffentlichen Schlüssel kann geprüft werden, ob Signaturen von Blöcken und damit die entsprechenden Blöcke selbst gültig sind. Öffentliche Schlüssel ursprünglicher Teilnehmer der ausgewählten Gruppe können beispielsweise in einem Genesisblock der Blockchain hinterlegt sein.

[0112] Bei der vorliegenden von einer der Zentralbank verwalteten Blockchain handelt es sich beispielsweise um eine öffentliche Blockchain, welche auf Blockchain-Servern der Zentralbank verwaltet wird. Beispielsweise erfolgt ein Eintragen neuer Blöcke ausschließlich durch diese von der Zentralbank verwalteten Blockchain-Server. In diesem Fall können beispielsweise rechenintensiven Prozess bei Hinzufügen zusätzlicher Blöcke entfallen. Beispielsweise ist für ein hinzufügen zusätzlicher Blöcke lediglich eine Signatur mit einem der Zentralbank zugeordneten Signaturschlüssel notwendig.

[0113] Ein Konsens kann auch auf andere Weise in einer Blockchain implementiert werden. So kann etwa ein Konsens erreicht werden, indem über eine Aufnahme vorgeschlagener Einträge in die Blockchain abgestimmt wird. Beispielsweise führt jeder Teilnehmer bzw. Blockchain-Server eine eindeutige Liste anderer Teilnehmer, welchen er als Gruppe vertraut. Jeder Teilnehmer kann zusätzliche Einträge vorschlagen, die in einen zusätzlichen Block der Blockchain aufgenommen werden sollen. Über die Aufnahme und damit die Anerkennung der Gültigkeit der vorgeschlagenen Einträge wird abgestimmt. So stimmt beispielsweise jeder Teilnehmer nur über diejenigen Vorschläge ab, welche von Teilnehmer seiner Liste stammen. Mit anderen Worten werden für die Entscheidung, ob ein Vorschlag für einen zusätzlichen Eintrag als gültig anerkannt wird, d.h. ob bezüglich der Gültigkeit dieses Eintrages ein Konsens zwischen den Teilnehmern besteht, nur die Stimmen derjenigen Teilnehmer berücksichtigt, die von der Liste desjenigen Teilnehmers umfasst sind, der den entsprechenden Vorschlag macht. Damit ein Vorschlag für einen Eintrag als gültig angenommen wird, muss ein bestimmter Minimumanteil an stimmberechtigten Teilnehmern mit Ja stimmen, beispielsweise 80%, 90%, 95% oder 100%. Alle vorgeschlagenen Einträge, die dieses Kriterium erfüllen, werden in die Blockchain aufgenommen. Eine solche Abstimmung kann mehrere Runden umfassen. Alle anderen Vorschläge, die das zuvor genannte Kriterium nicht erfüllen, werden verworfen oder bei der Abstimmung über den nächsten Block der Blockchain erneut zur Abstimmung gestellt. Die zuvor genannten Listen stellen Untergruppen des Blockchain-Netzwerks dar, denen der Teilnehmer, welcher die jeweilige Liste führt, als Gruppe insgesamt traut, ohne dass dies erfordert, dass er jedem einzelnen Teilnehmer der Liste traut. Ein Beispiel für ein solches Konsensverfahren bietet der Ripple Protokoll Konsens Algorithmus (David Schwartz et al.: „The Ripple Protocol Consensus Algorithm“, Ripple Labs Inc., 2014, https://ripple.com/files/ripple_consensus_whitepaper.pdf).

[0114] Nach Ausführungsformen wird die Banknote auf einen Empfang einer Bestellung von einer die Banknote ausgebenden Zentralbank hin hergestellt. Nach Ausführungsformen wird eine Angabe des vordefinierten Bereichs von Seriennummern empfangen. Nach Ausführungsform wird eine Angabe des für die Banknote vorgesehenen initialen Nominalwerts empfangen.

[0115] Ausführungsformen umfassen ein Verfahren zum Verwenden einer Banknote. Die Banknote umfasst ein Sicherheitselement mit einem Prozessor und einem Speicher. In dem Speicher des Sicherheitselements ist eine Identifikationsnummer der Banknote gespeichert, welche ein von einer die Banknote ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote individuell zugeordnetes anonymes Banknotenkonto identifiziert. In einem geschützten Speicherbereich des Speichers des Sicherheitselements ist ein banknotenindividueller kryptographischer Schlüssel gespeichert.

[0116] Das Verfahren zum Zahlen mit der Banknote umfasst:

- Empfangen einer Zahlungsanfrage für eine Zahlung mit der Banknote,
- Erzeugen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote, wobei das Kryptogramm aus der Identifikationsnummer der Banknote und einem zahlungsindividuellen Code als Eingangswerte

unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt wird,

• Senden einer das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung.

[0117] Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer der Banknote. Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe der Identifikationsnummer. Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe eines der Banknote zugeordneten initialen Nominalwerts.

[0118] Ausführungsformen können den Vorteil haben, dass die Banknote, wie bereits zuvor beschrieben, nicht zur für eine Bargeldzahlung, sondern zudem für eine bargeldlose Zahlung verwendet werden kann.

[0119] Nach Ausführungsformen handelt es sich bei der zum Zahlen verwendeten Banknote um eine Banknote nach einer der zuvor beschriebenen Ausführungsformen.

[0120] Nach Ausführungsformen gibt die Zahlungsanfrage einen zu zahlenden Betrag an. Das Verfahren zum Zahlen umfasst ferner ein Abgleichen des zu zahlenden Betrags mit einem in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwert der Banknote. Das zahlungsindividuelle Kryptogramm zum Autorisieren der Zahlung wird nur unter der Voraussetzung erzeugt, dass der gespeicherte aktuelle Nominalwert der Banknote größer oder gleich dem zu zahlenden Betrag ist. Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann, dass die Banknote über einen ausreichenden Nominalwert zur Ausführung der Zahlung verfügt.

[0121] Nach Ausführungsformen umfasst das Verfahren ferner zum Aktualisieren des gespeicherten aktuellen Nominalwerts der Banknote:

• Empfangen einer Aktualisierungsanfrage zum Aktualisieren des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote, wobei die Aktualisierungsanfrage einen aktualisierten Nominalwert der Banknote zusammen mit einer kryptographisch gesicherten Bestätigung der Zentralbank für den aktualisierten Nominalwert umfasst,

• Prüfen der kryptographisch gesicherten Bestätigung unter Verwendung eines in dem Speicher des Sicherheitselements gespeicherten kryptographischen Prüfschlüssels,

• im Falle einer erfolgreichen Prüfung, Ersetzten des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote mit dem empfangenen aktualisierten Nominalwert.

[0122] Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann, dass die Banknote über Kenntnis des ihr zugeordneten aktuellen Nominalwert gemäß Banknotenkonto verfügt.

[0123] Nach Ausführungsformen umfasst das Verfahren ferner zum Ausgeben des gespeicherten aktuellen Nominalwerts der Banknote:

• Empfangen einer Ausgabeanfrage zum Ausgeben des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote,

• in Antwort auf die Anfrage, Senden des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote.

[0124] Ausführungsformen können den Vorteil haben, dass der in der Banknote gespeicherte aktuelle Nominalwert direkt abgefragt werden kann und somit Kenntnis über diesen erhalten werden kann. Die Abfrage kann beispielsweise unter Verwendung eines Terminals oder, falls vorhanden, unter Verwendung einer Nutzerschnittstelle der Banknote erfolgen. Die Antwort wird beispielsweise an das Terminal oder an eine Anzeigevorrichtung der Nutzerschnittstelle zum Anzeigen gesendet.

[0125] Nach Ausführungsformen ist in dem Speicher des Sicherheitselements ferner die Seriennummer der Banknote gespeichert, welche zusammen mit dem gespeicherten aktuellen Nominalwert der Banknote gesendet wird und dem Empfänger des aktuellen Nominalwerts als Identifikator der Banknote für eine Bestätigungsanfrage an die Zentralbank zum Bestätigen des empfangenen aktuellen Nominalwerts der Banknote dient.

[0126] Ausführungsformen können den Vorteil haben, dass der ausgegebene aktuelle Nominalwert der Banknote durch die Zentralbank bestätigt werden kann.

[0127] Ausführungsformen umfassen ein Verfahren zur Zahlungsabwicklung unter Verwenden eines Terminals. Die Zahlung erfolgt mit einer Banknote, welche eine Kommunikationsschnittstelle zur Kommunikation mit dem Terminal und ein Sicherheitselement mit einem Prozessor und einem Speicher umfasst. In dem Speicher des Sicherheitselements ist eine Identifikationsnummer der Banknote gespeichert, welche ein von einer die Banknote ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote individuell zugeordnetes anonymes Banknotenkonto iden-

tifiziert. In einem geschützten Speicherbereich des Speichers des Sicherheitselements ist ein banknotenindividueller kryptographischer Schlüssel gespeichert. Das Terminal umfasst einen Prozessor, einen Speicher und eine Kommunikationsschnittstelle zu Kommunikation mit der Banknote.

[0128] Das Verfahren zur Abwicklung eines Zahlungstransfers durch das Terminal umfasst:

- Senden einer Zahlungsanfrage an die Banknote,
- Empfangen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote, wobei das Kryptogramm aus der Identifikationsnummer der Banknote und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt ist,
- Weiterleiten des zahlungsindividuellen Kryptogramms mit einer Angabe des zu zahlenden Betrags an die ausgebende Zentralbank für eine Validierung des zahlungsindividuellen Kryptogramms, eine Registerprüfung, ob der aktuelle Nominalwert der Banknote größer oder gleich dem zu zahlenden Betrag ist, und einer Ausführung des Zahlungstransfers,
- falls der Zahlungstransfer auf eine erfolgreiche Validierung und Registerprüfung durch die Zentralbank hin erfolgreich ausgeführt ist, Empfangen einer Bestätigung über den erfolgreichen Zahlungstransfer.

[0129] Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer der Banknote. Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe der Identifikationsnummer. Nach Ausführungsformen umfasst die Banknote beispielsweise eine visuelle Angabe eines der Banknote zugeordneten initialen Nominalwerts.

[0130] Ausführungsformen können den Vorteil haben, dass die Banknote, wie bereits zuvor beschrieben, nicht zur für eine Bargeldzahlung, sondern zudem für eine bargeldlose Zahlung verwendet werden kann.

[0131] Nach Ausführungsformen handelt es sich bei der zur Zahlungsabwicklung verwendeten Banknote um eine Banknote nach einer der zuvor beschriebenen Ausführungsformen.

[0132] Ausführungsformen können den Vorteil haben, dass die Zentralbank, neben ihrer Rolle als die Banknote ausgebende Institution, zusätzlich gegenüber der Banknote und/oder dem Terminal bzw. einem das verwenden Zahlungsempfänger Dienstleitungen im Bereich des Zahlungsverkehrs bzw. der Zahlungsabwicklung bereitstellt und mithin als eine klassische Bank bzw. eine Geschäftsbank auftritt.

[0133] Unter einer Zentralbank wird hier eine nationale oder supranationale Institution verstanden, welche über das Monopolrecht verfügt, Münzen und Banknoten als gesetzliche Zahlungsmittel auszugeben. Ferner kann eine Zentralbank geld- und währungspolitische Aufgaben wahrnehmen. Beispielsweise hält eine Zentralbank die Währungsreserve eines Währungsraumes, beispielsweise reguliert sie die Geldmenge, beispielsweise beeinflusst sie die Geldschöpfung durch Kreditvergabe der Geschäftsbanken und/oder refinanziert diese Geschäftsbanken und den Staat. Beispielsweise emittiert die Zentralbank die Banknoten und bringen diese in Umlauf.

[0134] Bei dem Terminal kann es sich beispielsweise um ein Terminal eines Verkäufers an einem Verkaufsort (engl.: „Point of Sale“/PoS), d.h. an dem Ort, an dem ein Verkauf vollzogen wird, handeln. Bei dem Terminal kann es sich ferner um ein Terminal handeln, welches an ein Nutzercomputersystem angeschlossen ist, über welches eine Zahlung mit der Banknote abgewickelt werden soll. Beispielsweise handelt es sich hierbei um eine Zahlungsabwicklung über ein Netzwerk, etwa das Internet, gegenüber einem Dienstanbieter, sei es ein Verkäufer oder ein Zahlungsdienstanbieter. Ebenso könnte das Terminal in Form eines mobilen tragbaren Kommunikationsgeräts, etwa einem Smartphone, eines Nutzers bereitgestellt werden. Der Nutzer könnte das mobile tragbare Kommunikationsgerät beispielsweise für eine Zahlungsabwicklung über ein Netzwerk, etwa das Internet, gegenüber einem Dienstanbieter nutzen, sei es ein Verkäufer oder ein Zahlungsdienstanbieter.

[0135] Nach Ausführungsformen werden mit dem zahlungsindividuellen Kryptogramm ferner die Seriennummer und/oder Identifikationsnummer der Banknote an die ausgebende Zentralbank gesendet. Ausführungsformen können den Vorteil haben, dass die Zentralbank das Kryptogramm einer Banknote bzw. einem Banknoten Konto zuordnen kann. Die Seriennummer und/oder Identifikationsnummer der Banknote werden beispielsweise in Klartext an die ausgebende Zentralbank gesendet.

[0136] Nach Ausführungsformen wird die Seriennummer und/oder Identifikationsnummer der Banknote zusammen mit dem zahlungsindividuellen Kryptogramm empfangen.

[0137] Nach Ausführungsformen wird mit dem zahlungsindividuellen Kryptogramm ferner der zahlungsindividuelle Code empfangen und mit dem zahlungsindividuellen Kryptogramm an die ausgebende Zentralbank gesendet. Ausführungsformen können den Vorteil haben, dass zahlungsindividuelle Code zur

Validierung des Kryptogramms verwendet werden kann. Der zahlungsindividuelle Code wird beispielsweise in Klartext an die ausgebende Zentralbank gesendet.

[0138] Nach Ausführungsformen verfügt die ausgebende Zentralbank über einen Prüfschlüssel zum Prüfen der Validität des zahlungsindividuellen Kryptogramms. Bei dem banknotenindividuellen kryptographischen Schlüssel handelt es sich beispielsweise um einen symmetrischen kryptographischen Schlüssel und bei dem Prüfschlüssel um denselben einen symmetrischen kryptographischen Schlüssel. Bei dem banknotenindividuellen kryptographischen Schlüssel handelt es sich beispielsweise um einen privaten kryptographischen Schlüssel und bei dem Prüfschlüssel um einen dem privaten kryptographischen Schlüssel der Banknote zugeordneten öffentlichen kryptographischen Schlüssel desselben asymmetrischen Schlüsselpaars.

[0139] Nach Ausführungsformen verwendet die ausgebende Zentralbank die Identifikationsnummer der Banknote zum Ermitteln der Seriennummer der Banknote, beispielsweise durch eine Registerabfrage, beispielsweise des zweiten Registers.

[0140] Nach Ausführungsformen verwendet die ausgebende Zentralbank die Identifikationsnummer und/oder die Seriennummer zum Ermitteln des aktuellen Nominalwerts der Banknote. Beispielsweise umfasst das Ermitteln Registerabfragen, beispielsweise des ersten und/oder zweiten Registers.

[0141] Nach Ausführungsformen wird ferner eine Identifikationsnummer eines Empfängerkontos zum Empfangen des zu zahlenden Betrags an die ausgebende Zentralbank gesendet. Ausführungsformen können den Vorteil haben, dass die Zentralbank die Zahlung von der Banknote bzw. dem der Banknote zugeordneten Banknotenkonto an das Empfängerkonto ausführen kann.

[0142] Nach Ausführungsformen verwendet die ausgebende Zentralbank die Identifikationsnummer des Empfängerkontos, um den zu zahlenden Betrag auf eine erfolgreiche Validierung des zahlungsindividuellen Kryptogramms und eine erfolgreiche Registerprüfung erfolgreiche hin von dem durch die ausgebende Zentralbank verwalteten und der entsprechenden Banknote individuell zugeordneten anonymen Banknotenkontos an das Empfängerkonto zu transferieren. Beispielsweise könne so Zahlungen von einem Banknotenkonto an ein anderes ausgeführt werden.

[0143] Nach Ausführungsformen ist die Bestätigung des Zahlungstransfers kryptographisch gesichert und das Verfahren umfasst ferner ein Prüfen der Bestätigung unter Verwendung eines kryptographischen Prüfschlüssels. Nach Ausführungsformen handelt es sich bei dem kryptographischen Prüfschlüssel zum Prüfen der Bestätigung des Zahlungstransfers beispielsweise einen öffentlichen kryptographischen Schlüssel eines der Zentralbank zugeordneten asymmetrischen Schlüsselpaars.

[0144] Nach Ausführungsformen umfasst die Bestätigung des Zahlungstransfers eine Angabe des aktualisierten Nominalwerts der Banknote zusammen mit einer kryptographisch gesicherten Bestätigung der Zentralbank für den aktualisierten Nominalwert. Ausführungsformen können den Vorteil haben, dass mit der Bestätigung des Zahlungstransfers zugleich eine Bestätigung über den aktualisierten Nominalwert bereitgestellt und beispielsweise an die Banknote zum Aktualisieren des gespeicherten Nominalwerts weitergeleitet werden kann.

[0145] Nach Ausführungsformen aktualisiert die ausgebende Zentralbank den Nominalwert der Banknote in einem Register. Nach Ausführungsformen handelt es sich bei dem aktualisierten Nominalwert um den bisherigen Nominalwert der Banknote abzüglich des gezahlten Betrags. Beispielsweise kann anhand Registers, etwa des ersten Registers, der Nominalwert einer Banknote eingesehen werden.

[0146] Nach Ausführungsformen umfasst das Verfahren ferner ein Senden einer Aktualisierungsanfrage zum Aktualisieren des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote. Die Aktualisierungsanfrage umfasst den aktualisierten Nominalwert der Banknote zusammen mit der kryptographisch gesicherten Bestätigung der Zentralbank für den aktualisierten Nominalwert. Ausführungsformen können den Vorteil haben, dass die Banknote so zum Aktualisieren des gespeicherten Nominalwerts veranlasst werden kann.

[0147] Nach Ausführungsformen ersetzt die Banknote den in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts mit dem empfangenen aktualisierten Nominalwert unter der Voraussetzung, dass die Prüfung der kryptographisch gesicherten Bestätigung unter Verwendung eines in dem Speicher des Sicherheitselements gespeicherten kryptographischen Prüfschlüssels erfolgreich ist. Nach Ausführungsformen handelt es sich bei dem kryptographischen Prüfschlüssel um den banknotenindividuellen kryptographischen Schlüssel, beispielsweise um einen symmetrischen kryptographischen Schlüssel. Nach Ausführungsformen handelt es sich bei dem kryptographischen Prüfschlüssel um einen zusätzlichen zu dem banknotenindividuellen kryptographischen Schlüssels gespeicherten kryptographischen Prüfschlüssel, beispielsweise einen öffentlichen kryptographischen Schlüssel eines der Zentralbank zugeordneten asymmetrischen Schlüsselpaars.

[0148] Nach Ausführungsformen umfasst die kryptographisch gesicherte Bestätigung den verschlüsselten aktualisierten Nominalwert. Nach Ausführungsformen ist der aktualisierte Nominalwert zusammen mit der Identifikationsnummer oder der Seriennummer der Banknote verschlüsselt. Nach Ausführungsformen ist der aktualisierte Nominalwert zusammen mit einem Zeitstempel verschlüsselt. Nach Ausführungsformen wurde zunächst eine Hashfunktion auf die zu verschlüsselnden Daten angewendet und der resultierende Hashwert verschlüsselt. Ausführungsformen können den Vorteil haben, dass die Übertragung des aktualisierten Nominalwerts so in kryptographisch gesicherter Weise erfolgen und eindeutig der Banknote zugeordnet werden kann. Mittels des Zeitstempels kann zudem sichergestellt werden, dass es sich tatsächlich um einen aktuellen Nominalwert bzw. einen Nominalwert handelt, welcher aktueller als ein gespeicherter Nominalwert ist. Beispielsweise speichert die Banknote den aktuellen Nominalwert zusammen mit einem dem Nominalwert zugeordneten Zeitstempel. Beispielsweise ersetzt die Banknote bei einem Ersetzen des Nominalwerts durch einen aktualisierten Nominalwert im Zuge einer Aktualisierung auch den bisher gespeicherten Zeitstempel durch einen aktualisierten Zeitstempel, welcher dem aktualisierten Nominalwert zugeordnet ist. Beispielsweise prüft die Banknote vor einem Aktualisieren des gespeicherten Nominalwerts, ob ein Zeitstempel eines zum Aktualisieren bereitgestellten Nominalwerts tatsächlich aktueller als der gespeicherte Zeitstempel des bisherigen Nominalwerts ist. Somit kann sichergestellt werden, dass es sich bei dem zum Aktualisieren verwendet Zeitstempel tatsächlich um einen aktuelleren Zeitstempel handelt.

[0149] Nach Ausführungsformen wird die kryptographisch gesicherte Bestätigung ferner zusammen mit der Identifikationsnummer der Banknote, der Seriennummer der Banknote und/oder dem Zeitstempel empfangen. Ausführungsformen können den Vorteil haben, dass die kryptographisch gesicherte Bestätigung eindeutig der Banknote zugeordnet werden kann.

[0150] Nach Ausführungsformen umfasst die Banknote eine Mehrzahl von Sicherheitsmerkmalen. Das Verfahren umfasst als Voraussetzung für das Senden der Zahlungsanfrage ein erfolgreiches Erfassen und Validieren von ein oder mehreren vordefinierenden Sicherheitsmerkmalen der Mehrmals von Sicherheitsmerkmalen der Banknote. Ausführungsformen können den Vorteil haben, dass die Banknote anhand der Sicherheitsmerkmale auf ihre Authentizität und Validität geprüft werden kann.

[0151] Nach Ausführungsformen wird eine Mehrzahl von Banknoten empfangen. Für jede der Banknoten wird jeweils ein aktueller Nominalwert ermittelt. Aus der Mehrzahl von empfangenen Banknoten wird ein Satz von Banknoten ausgewählt und einbehalten, deren aufsummierte aktuelle Nominalwerte einen Betrag ergeben, der kleiner als ein zu zahlender Betrag ist. Ein verbleibender Differenzbetrag zwischen dem zu zahlenden Betrag und dem aufsummierten Betrag des Satzes von ausgewählten Banknoten ist kleiner als ein aktueller Nominalwert einer weiteren Banknote der Mehrzahl von Banknoten, welche nicht von dem Satz von ausgewählten Banknoten umfasst ist. Die Zahlungsanfrage zur Zahlung des Differenzbetrags wird an die weitere Banknote gesendet.

[0152] Ausführungsformen können den Vorteil haben, dass eine Kombination aus bargeldbasierter und bargeldloser Zahlung ermöglicht werden könnte. Für den einbehaltenen Satz von Banknoten ergibt sich keine Notwendigkeit von Zahlungsautorisierung und/oder Zahlungen unter Verwendung der Banknotenkonten der entsprechenden Banknoten. Die Zahlung mit diesen Banknoten erfolgt vielmehr durch Übergabe der Banknoten, wie bei Bargeldzahlungen üblich. Falls der zu zahlende Betrag nicht aufgeht, d.h. die Summe der Nominalwerte der Banknoten des einbehaltenen Satzes von Banknoten kleiner als der zu zahlender Betrag ist und keine weitere Banknote vorliegt, deren Nominalwert dem Differenzbetrag entspricht, erfolgt die Zahlung des Differenzbetrags bargeldlos unter Verwendung einer weiteren Banknote, deren Nominalwert größer als der entsprechende Differenzwert ist. Alternativ kann die Zahlung des Differenzbetrags auch durch einbehalten der weiteren Banknote erfolgen und der überzählig bezahlte Betrag rückerstattet werden. Beispielsweise durch eine Transaktion von einem Konto, z.B. Banknotenkonto, des Zahlungsempfängers an ein Banknotenkonto einer nicht einbehaltenen Banknote, welche im Eigentum des Zahlungspflichtigen verbleibt. Nach Ausführungsformen werden alle nicht einbehaltenen Banknoten zurückgegebenen.

[0153] Nach Ausführungsformen umfassen die Banknoten der Mehrzahl von Banknoten jeweils eine Mehrzahl von Sicherheitsmerkmalen. Das Verfahren umfasst beispielsweise für jede der Banknoten jeweils eine Gültigkeitsprüfung. Die Gültigkeitsprüfung der Banknoten umfasst beispielsweise jeweils ein erfolgreiches Erfassen und Validieren von ein oder mehreren vordefinierenden Sicherheitsmerkmalen der Mehrmals von Sicherheitsmerkmalen der entsprechenden Banknote. Ausführungsformen können den Vorteil haben, dass die Authentizität und Validität aller Banknoten sichergestellt werden kann, insbesondere der einbehaltenen Banknoten.

[0154] Nach Ausführungsformen wird ein Verfahren zum Ersetzen einer beschädigten Banknote bereitgestellt. Die Banknote umfasst die visuelle Angabe der Seriennummer mehrfach über die Banknote verteilt. Weist die Banknote eine Beschädigung auf, umfasst

das Ersetzen der Banknote durch die die beschädigte Banknote ausgebende Zentralbank:

- Prüfen eines Beschädigungsgrads der Banknote,
- falls der Beschädigungsgrads der Banknote einen vordefinierten zulässigen maximalen Beschädigungsgrad nicht überschreitet, Erfassen der Seriennummer und/oder Identifikationsnummer der Banknote,
- Initialisieren einer Sperrung der der erfassten Seriennummer und/oder Identifikationsnummer zugeordneten Registereinträge,
- Ermitteln eines aktuellen Nominalwerts der Banknote unter Verwendung erfassten Seriennummer und/oder Identifikationsnummer,
- Auszahlen des aktuellen Nominalwerts der beschädigten Banknote.

[0155] Ausführungsformen können den Vorteil haben, dass im Falle einer Beschädigung der tatsächliche Nominalwert der Banknote ersetzt werden kann. Dieser tatsächliche Nominalwert kann deutlich von dem initialen Nominalwert der Banknote und/oder einem Mindestnominalwert der Banknote abweichen. Nach Ausführungsformen ist dafür, dass der Beschädigungsgrads der Banknote einen vordefinierten zulässigen maximalen Beschädigungsgrad nicht überschreitet, erforderlich, dass mehr als 50% der Banknote vorliegen und/oder die Banknote ein oder mehrere für ein Ersetzen notwendige valide Sicherheitsmerkmale umfasst.

[0156] Nach Ausführungsformen handelt es sich bei der ersetzten Banknote um eine Banknote nach einer der zuvor beschriebenen Ausführungsformen. Nach Ausführungsformen wird die beschädigte Banknote einbehalten.

[0157] Nach Ausführungsformen umfasst das Erfassen der Seriennummer ein Lesen der visuellen Angabe der Seriennummer unter Verwendung eines Sensors des Terminals. Nach Ausführungsformen umfasst das Erfassen der Seriennummer ein Empfangen der unter Verwendung der Kommunikationsschnittstelle der Banknote gesendeten Seriennummer unter Verwendung der Kommunikationsschnittstelle des Terminals.

[0158] Nach Ausführungsformen umfasst das Erfassen der Identifikationsnummer ein Empfangen der unter Verwendung der Kommunikationsschnittstelle der Banknote gesendeten Seriennummer unter Verwendung der Kommunikationsschnittstelle des Terminals.

[0159] Nach Ausführungsformen umfasst das Auszahlen des aktuellen Nominalwerts der beschädigten Banknote ein Bereitstellen ein oder mehrerer Banknoten als Ersatz, deren aktuelle Nominalwerte in der Summe dem aktuellen Nominalwert der beschädigten Banknote entsprechen. Nach Ausführungsformen handelt es sich bei den ein oder mehreren Banknoten als Ersatz um Banknoten nach einer der zuvor beschriebenen Ausführungsformen. Nach Ausführungsformen umfasst das Auszahlen des aktuellen Nominalwerts der beschädigten Banknote eine Transaktion eines Betrags in Höhe des aktuellen Nominalwerts von dem Bankkonto der beschädigten Banknote oder einem Bankkonto der die beschädigte Banknote ausgebenden Zentralbank an ein von einem Besitzer der beschädigten Banknote angegebenes Bankkonto. Beispielsweise ist das angegebene Banknotenkonto einer anderen Banknote des Besitzers der beschädigten Banknoten, dem Besitzer der beschädigten Banknote persönlich oder einer anderen von dem Besitzers der beschädigten Banknoten gewählten Institution zugeordnet.

[0160] Nach Ausführungsformen umfasst die Beschädigung eine Beschädigung des Sicherheitselements, sodass das Sicherheitselement keine zahlungsindividuellen Kryptogramme mehr bereitstellen kann. Beispielsweise ist der Prozessor, der Speicher und/oder eine Kommunikationsschnittstelle des Sicherheitselements beschädigt. Beispielsweise fehlt das Sicherheitselement.

[0161] Nach Ausführungsformen ist die Mehrzahl von visuellen Angaben der Seriennummer derart über die Banknote verteilt, dass sichergestellt werden kann, dass die Seriennummer und damit das Banknotenkonto der Banknote ermittelt werden kann, solange mehr als 50% der Banknote vorliegen. Nach Ausführungsformen ist die Mehrzahl von Sicherheitselementen derart über die Banknote verteilt, dass sichergestellt werden kann, dass für ein Ersetzen notwendige valide Sicherheitsmerkmale vorliegen, solange mehr als 50% der Banknote unbeschädigt vorliegen.

[0162] Nach Ausführungsformen umfasst das Ersetzen der Banknote durch die die beschädigte Banknote ausgebenden Zentralbank ferner einen Sperreintrag in einem von der ausgebenden Zentralbank verwalteten Sperrregister. Durch den Sperreintrag wird das Banknotenkonto der Banknote gesperrt. Im Falle eines Sperreintrag für das Banknotenkonto der Banknote durch die Zentralbank kann beispielweise sichergestellt werden, dass kein Geld von dem gesperrten Bankkonto auf ein anderes Konto, beispielsweise Banknotenkonto, transferiert werden kann, d.h. dass keine Zahlungen gesendet werden können, und/oder dass kein Geld von einer anderen Konto, beispielsweise Banknotenkonto, auf das gesperrte Bankkonto transferiert werden kann, d.h. dass keine Zahlungen empfangen werden können.

[0163] Beispielsweise umfasst das Sperren des Banknotenkontos der beschädigten Banknote eine

Transaktion eines noch verbleibenden Restbetrag auf dem Bankkonto der beschädigten Banknote an ein Konto der Zentralbank, beispielsweise ein Banknotenkonto einer andern sich im Besitz der Zentralbank befindenden Banknote. Dies kann den Vorteil haben, dass im Zuge eines Ersetzens einer beschädigten kein Restbetrag auf dem gesperrten Konto verbleibt.

[0164] Ausführungsformen könnten den Vorteil haben, dass bei einem Ersetzen der Banknote nicht der Prozessor und/oder das Sicherheitselement der beschädigten Banknote zurückgehalten und mit diesem nach dem Auszahlen des (letzten) aktuellen Nominalwerts der beschädigten Banknote weiterhin Zahlungen getätigt, d.h. Kryptogramme ausgegeben werden können. Ferner kann beispielsweise verhindert werden, dass versehentlich Zahlungen auf das Banknotenkonto der beschädigten Bankknote erfolgen, nachdem der (letzte) aktuellen Nominalwert bereits ausgezahlt und die beschädigte Banknote einbehalten wurde.

[0165] Beispielsweise wird bei einer Transaktion von einem Banknotenkonto einer Banknote als Voraussetzung zum Ausführen der Transaktion von der Zentralbank geprüft, ob das entsprechende Banknotenkonto gesperrt ist, d.h. ein Speereintrag vorliegt. Falls das Banknotenkonto nicht gesperrt ist, wird die Transaktion ausgeführt. Falls das Banknotenkonto gesperrt ist, wird die Transaktion nicht ausgeführt.

[0166] Beispielsweise wird bei einer Transaktion auf ein Banknotenkonto einer Banknote als Voraussetzung zum Ausführen der Transaktion von der Zentralbank geprüft, ob das entsprechende Banknotenkonto gesperrt ist, d.h. ein Speereintrag vorliegt. Falls das Banknotenkonto nicht gesperrt ist, wird die Transaktion ausgeführt. Falls das Banknotenkonto gesperrt ist, wird die Transaktion nicht ausgeführt.

[0167] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Fig. 1 schematische Blockdiagramme exemplarischer Banknoten,

Fig. 2 ein schematisches Blockdiagramm eines exemplarischen Systems mit einer exemplarischen Banknote,

Fig. 3 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Ausstellen von Banknoten,

Fig. 4 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Zahlungsabwicklung mit einem Terminal,

Fig. 5 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Bestätigung eines aktuellen Nominalwerts einer Banknote,

Fig. 6 ein schematisches Blockdiagramm eines exemplarischen Verfahrens zum Verwenden von Banknoten,

Fig. 7 ein schematisches Flussdiagramm exemplarischer Verfahren zum Verwenden einer Banknote,

Fig. 8 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Aktualisieren eines Nominalwerts einer Banknote,

Fig. 9 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Ausgeben eines Nominalwerts einer Banknote,

Fig. 10 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Ausstellen einer Banknote,

Fig. 11 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Zahlungsabwicklung mit einem Terminal, und

Fig. 12 ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Zahlungsabwicklung mit einer Mehrzahl von Banknoten.

[0168] Elemente der nachfolgenden Ausführungsformen, die einander entsprechen, werden mit denselben Bezugszeichen gekennzeichnet.

[0169] **Fig. 1A** und **Fig. 1B** zeigen exemplarische Banknoten **100**. Die in **Fig. 1A** gezeigte Banknote **100** umfasst eine Mehrzahl von Sicherheitsmerkmale **110**, welche die Authentizität und Validität der Banknote **100** belegen. Die Sicherheitsmerkmale **110** sind über die Banknote **100** verteilt angeordnet. Beispielsweise sind die Sicherheitsmerkmale **110** so über die Banknote **100** verteilt angeordnet, dass solange mehr als 50% der Banknote in unbeschädigtem Zustand vorliegen, die Authentizität und Validität der Banknote **100** nachgewiesen werden kann. Die Banknote **100** umfasst ferner eine visuelle Angabe der Seriennummer **106** der Banknote **100**, welche beispielsweise auf die Banknote **100** aufgedruckt ist. Beispielsweise umfasst die Banknote **100** eine Mehrzahl von visuellen Angaben der Seriennummer **106**, welche über die Banknote **100** verteilt angeordnet sind, etwa in Mikroschrift. Beispielsweise ist die Seriennummer **106** so über die Banknote **100** verteilt angeordnet, dass solange mehr als 50% der Banknote in unbeschädigtem Zustand vorliegen, die Seriennummer **106** der Banknote **100** bestimmt werden kann. Die Seriennummer **106** dient beispielsweise der Identifikation der Banknote **100** und kann einem aktuellen Nominalwert der Banknote, etwa dem Kontostand eines Banknotenkontos und/oder einer Identifikationsnummer des Banknotenkontos der Banknote **100** zugeordnet sein. So kann unter Verwendung der Seriennummer **106** der Banknote **100** beispielsweise der aktuelle Nominalwert der Banknote **100** bestimmt werden.

[0170] Ferner umfasst die Banknote ein oder mehrere visuelle Angaben eines initialen Nominalwerts **108** der Banknote **100**. Bei dem initialen Nominalwerts **108** handelt es sich beispielsweise um einen Mindestnominalwert der Banknote **100**. Beispielsweise umfasst die Banknote **100** ein oder mehrere visuelle Angaben eines von dem initialen Nominalwert **108** verschiedenen Mindestnominalwerts zusätzlich zu der Angabe des initialen Nominalwerts **108**. Beispielsweise umfasst die Banknote **100** die ein oder mehreren visuellen Angaben des Mindestnominalwerts anstelle von visuellen Angaben eines von dem Mindestnominalwert verschiedenen initialen Nominalwert **108**. Zusätzlich umfasst die Banknote ein Sicherheitselement **102** mit einem Prozessor und einem Speicher. In dem Speicher des Sicherheitselements **102** ist eine Identifikationsnummer der Banknote **100** gespeichert. Die Identifikationsnummer identifiziert ein von einer die Banknote **100** ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote **100** individuell zugeordnetes anonymes Banknotenkonto. In einem geschützten Speicherbereich des Speichers ist ein banknotenindividueller kryptographischer Schlüssel gespeichert, beispielsweise in Form eines symmetrischen oder eines privaten kryptographischen Schlüssels. Den banknotenindividuellen kryptographischen Schlüssel verwendet die Banknote **100** zum Erzeugen von zahlungsindividuellen Kryptogrammen zur Autorisierung von bargeldlosen Zahlungen mit der Banknote **100**. Bei solchen bargeldlosen Zahlungen handelt es sich um Transaktion von dem Banknotenkonto der Banknote **100** an ein Bankkonto, z. B. Banknotenkonto, eines Zahlungsempfängers. Die Kryptogramme werden jeweils aus der Identifikationsnummer der Banknote **100** und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt. Der zahlungsindividuelle Code umfasst die individuelle Zahlung charakterisierende Angaben, wie etwa eine Zeitangabe, eine Angabe des zu zahlenden Betrags und/oder eine Angabe des Empfängers/Empfängerkontos.

[0171] Ferner umfasst die Banknote eine Kommunikationsschnittstelle **104** zum Kommunizieren mit einem Terminal, insbesondere zu einem kontaktlosen Kommunizieren. Über die Kommunikationsschnittstelle **104** empfängt die Banknote **100** beispielsweise Zahlungsanfragen und sendet beispielsweise Zahlungsautorisierungen mit zahlungsindividuellen Kryptogrammen. Ferner könnten die Banknote **100** visuelle Angaben der Identifikationsnummer der Banknote **100** umfassen.

[0172] **Fig. 1B** zeigt eine exemplarische Banknote **100**, welche der exemplarischen Banknote **100** aus **Fig. 1A** entspricht. Zusätzlich umfasst die Banknote **100** in **Fig. 1B** eine Nutzerschnittstelle **112**. Die Nutzerschnittstelle **112** umfasst beispielsweise eine Eingabe- und/oder eine Ausgabevorrichtung der Banknote **100**. Beispielsweise umfasst die Nutzerschnittstelle **112** ein Touchpad zur Eingabe von Daten, etwa Transaktionsdaten, in die Banknote **100** und/oder ein Display zur Anzeige von Daten, etwa Transaktionsdaten, welche die Banknote **100** verarbeiten soll oder verarbeitet hat. Beispielsweise umfasst die Nutzerschnittstelle **112** ein Touch-Display, mit welchem sowohl Daten von dem Nutzer eingegeben werden können, als auch dem Nutzer Daten angezeigt werden können.

[0173] **Fig. 2** zeigt ein exemplarisches System mit einer exemplarischen Banknote **100**. Die Banknote **100** umfasst ein Sicherheitselement **102** mit einem Prozessor **124** und einem Speicher **120**. Der Prozessor **124** für Programminstruktionen **128** aus. Diese Programminstruktionen **128** umfassen beispielsweise kryptographische Programminstruktionen zum Erzeugen zahlungsindividueller Kryptogramme. Ferner können die kryptographischen Programminstruktionen beispielsweise dazu konfiguriert sein, kryptographische Schlüssel zu erzeugen. In dem Speicher **120** ist eine Identifikationsnummer **116** eines Banknotenkontos der Banknote **100** („banknote account number“/BAN) gespeichert. Ferner ist in dem Speicher **120** beispielsweise die Seriennummer der106 der Banknote **100** und/oder ein aktueller Nominalwert **109** Banknote **100** der gespeichert. In einem geschützten Speicherbereich **122** des Speichers **120** ist ein banknotenindividueller kryptographischer Schlüssel **118** der Banknote zum Erzeugen zahlungsindividueller Kryptogramme gespeichert. Ferner umfasst die Banknote **100** beispielsweise eine Kommunikationsschnittstelle **104** zur Kommunikation mit externen Geräten, wie etwa einer einem Terminal **130**. Die Kommunikationsschnittstelle **104** ist beispielsweise für eine kontaktlose Nahfeldkommunikation konfiguriert. Zusätzlich umfasst die Banknote **100** visuelle Angaben **107**, etwa der Seriennummer **106** und/oder Identifikationsnummer **116**. Ferner kann die Banknote **100** beispielsweise ferner eine Nutzerschnittstelle mit einer Eingabe- und/oder Ausgabevorrichtung zum Eingeben und/oder Anzeigen von Daten umfassen, wie etwa Transaktionsdaten.

[0174] Die Banknote **100** kommuniziert unter Verwendung der Kommunikationsschnittstelle **104** beispielsweise mit einem Terminal **130**. Das Terminal **130** ist beispielsweise ein Zahlungsterminal eines PoS. Das Terminal **130** umfasst einen Prozessor **134** zum Ausführen von Programminstruktionen **136** und einen Speicher **132**. Ferner umfasst das Terminal **130** eine Kommunikationsschnittstelle **137** zur Kommunikation mit der Banknote **100**. Zusätzlich umfasst das Terminal **130** eine Kommunikationsschnittstelle **139** zur Kommunikation über ein Netzwerk **160**, wie etwa das Internet. Das Terminal **130** ist beispielsweise zu einer Zahlungsabwicklung mit der Banknote **100** konfiguriert. Hierzu sendet das Terminal **130**

beispielsweise eine Zahlungsanfrage an die Banknote **100** und empfängt eine Zahlungsautorisierung mit einem zahlungsindividuellen Kryptogramm von der Banknote **100**, welche das Terminal **130** über das Netzwerk **160** an einen Zentralbankserver **220** eines Zentralbanksystems **156** zum Ausführen in Form einer Transaktion von dem der Banknote **100** zugeordneten Banknotenkonto an ein Empfängerkonto des Empfängers der Zahlung. Ferner kann das Terminal beispielsweise Sensor **139** umfassen. Der Sensor **139** ist beispielsweise dazu konfiguriert visuelle Angabe **107** der Banknote **100** zu erfassen, wie etwa die Seriennummer **106**. Ferner kann der Sensor **139** beispielsweise zum Erfassen von Sicherheitsmerkmalen der Banknote **100** konfiguriert sein, um deren Authentizität und Validität zu prüfen. In dem Speicher **132** ist beispielsweise ein Identifikator bzw. eine Identifizierungsnummer eines Kontos gespeichert, welche das Terminal **130** als Empfängerkonto zum Empfangen von Zahlungen verwendet.

[0175] Das Terminal **130** kommuniziert beispielsweise über einen Remoteserver **170** mit dem Zentralbankserver **220**. Der Server **170** umfasst beispielsweise einen Speicher **172**, einen Prozessor **174** zum Ausführen von Programminstruktionen **176** und eine Kommunikationsschnittstelle **178** zur Kommunikation über das Netzwerk **160**. Beispielsweise stellt der Server **170** dem Terminal **130** den Identifikator eines als Empfängerkonto verwendeten Kontos oder Banknotenkontos zur Verfügung. Beispielsweise leitet der Server **170** über das Terminal **130** empfangene Zahlungsautorisierungen an den Zentralbankserver **220** weiter. Beispielsweise leitet der Server **170** von dem Zentralbankserver **220** empfangene Zahlungsbestätigungen an das Terminal **130** weiter.

[0176] Das System umfasst ferner einen Zentralbankserver **220** mit einem Speicher **222** und einem Prozessor **224** zum Ausführen von Programminstruktionen **226**. Ferner umfasst der Zentralbankserver **220** beispielsweise eine Kommunikationsschnittstelle **228** zur Kommunikation über das Netzwerk **160**. Der Zentralbankserver **220** ist beispielsweise dazu konfiguriert Autorisierungsanfragen mit zahlungsindividuellen Kryptogrammen zur Autorisierung von Zahlungen unter Verwendung von Banknotenkonten von Banknoten **100** zu prüfen und, im Falle erfolgreicher Prüfungen, die autorisierten Zahlungen auszuführen. Sind die Zahlungen ausgeführt, sendet der Zentralbankserver **220** beispielsweise Zahlungsbestätigungen. Die Zahlungsbestätigungen umfassen beispielsweise Angaben zu aus den Zahlungen resultierenden aktuellen Nominalwerten der Banknoten. Ferner ist der Zentralbankserver **220** beispielsweise dazu konfiguriert im Zuge einer Herstellung einer Banknote **100** ein banknotenindividuelles Banknotenkonto für die entsprechende Banknote **100** einzurichten und/oder ein eingerichtetes Banknotenkonto zu sperren, etwa falls eine beschädigte Banknote von der Zentralbank aus dem Verkehr genommen wird. Ferner kann der Zentralbankserver **220** oder ein anderes mit dem Zentralbankserver in Kommunikationsverbindung stehendes Computersystem des Zentralbanksystems einen Sensor zum Prüfen von Sicherheitsmerkmalen beschädigter Banknote umfassen. Falls die Prüfung der Sicherheitsmerkmalen sowie des Beschädigungsgrads der Banknote ergibt, dass es sich um eine valide Banknote handelt, ersetzt die Zentralbank die beschädigte Banknote. Hierzu ermittelt der Zentralbankserver **220** beispielsweise den aktuellen Nominalwert der beschädigten Banknote unter Verwendung einer entsprechenden Anfrage die von der Zentralbank verwalteten Register **148**, **150**, zahlt den aktuellen Nominalwert aus und sperrt das Banknotenkonto der beschädigten Banknote. Beispielsweise erfolgt ein Sperreintrag in ein der mehren der Register **148**, **150**.

[0177] Das Zentralbanksystem **156** umfasst ferner die Register **148**, **150**. Das Register **148** umfasst beispielsweise Zuordnungen der Seriennummern der einzelnen Banknoten **100** zu der jeweiligen Identifikationsnummern des Banknotenkontos der entsprechenden Banknote. Ferner kann das Register den Identifikationsnummern der Banknotenkontos der einzelnen Banknoten **100** jeweils einen kryptographischen Prüfschlüssel zum Prüfen von Kryptogrammen der entsprechenden Banknote **100** zuordnen. Das Register **150** ist beispielsweise als eine Look-Up-Tabelle konfiguriert, und umfasst beispielsweise Zuordnungen von aktuellen Nominalwerten der Banknoten **100** zu den Seriennummern der einzelnen Banknoten **100**. Beispielsweise kann unter Verwendung des Registers **150** ein aktueller Nominalwert einer Banknote **100** mit der Seriennummer der entsprechenden Banknote **100** als Datenbankzugriffsschlüssel abgefragt werden. Ferner kann das Zentralbanksystem **156** ein Buchungssystem zum Ausführen von Transaktionen unter Verwendung des Banknotenkontos der von der Zentralbank ausgegeben Banknoten **100** umfassen.

[0178] Anstelle des Terminals **130** kann zur Zahlungsabwicklung auch ein mobiles tragbares Kommunikationsgerät **180** oder ein Nutzercomputersystem **190**, etwa zur Zahlungsabwicklung über das Internet, verwendet werden. Dabei kann das mobile Kommunikationsgerät **180** oder der Nutzercomputersystem **190** beispielsweise als lokaler PoS dienen. Beispielsweise erfolgt die Zahlungsabwicklung unter Verwendung des Remoteserver **170**. Beispielsweise erfolgt die Zahlungsabwicklung unter Verwendung eines Servers **200** eines Zahlungsdienstanbieters bzw. eines Finanzdienstleisters, welcher als PsP fungiert.

[0179] Das mobile Kommunikationsgerät **180**, etwa ein Smartphone, umfasst beispielsweise einen Speicher **182** und einen Prozessor **184** zum Ausführen von Programinstruktionen **186**. Ferner umfasst das

mobile Kommunikationsgerät **180** beispielsweise eine Kommunikationsschnittstelle **187** zur Kommunikation mit der Banknote **100** sowie eine Kommunikationsschnittstelle **188** zur Kommunikation über das Netzwerk **160**. Beispielsweise umfasst das mobile Kommunikationsgerät **180** eine Kamera zum Erfassen von visuellen Angaben **107** der Banknote **100**, wie etwa der Seriennummer **106** der Banknote **100**. Das mobile Kommunikationsgerät **180** ist beispielsweise dazu konfiguriert eine Zahlungsanfrage, etwa von dem Server **170** oder dem Zahlungsdienstserver **200**, an die Banknote **100** und eine Zahlungsautorisierung der Banknote **100** mit einem zahlungsindividuellen Kryptogramm an den Server **170** oder den Zahlungsdienstserver **200** weiterzuleiten. Beispielsweise kann das mobile Kommunikationsgerät **180** dazu konfiguriert sein, direkt oder unter Vermittlung eines Servers wie dem Server **170** oder dem Zahlungsdienstserver **200** den aktuellen Nominalwert der Banknote **100** zu ermitteln und etwa einem Nutzer unter Verwendung einer Nutzerschnittstelle **181** anzuzeigen. Die Nutzerschnittstelle **181** umfasst beispielsweise eine Eingabe- und eine Ausgabevorrichtung zur Kommunikation des Nutzers mit dem mobilen Kommunikationsgerät **180**. Die Eingabevorrichtung umfasst beispielsweise eine Tastatur. Die Ausgabevorrichtung umfasst beispielsweise ein Display. Beispielsweise sind Eingabe- und Ausgabevorrichtung in Form eines Touch-Displays miteinander kombiniert.

[0180] Das Nutzercomputersystem **190** umfasst beispielsweise einen Speicher 192und einen Prozessor **194** zum Ausführen von Programinstruktionen **196**. Ferner umfasst das Nutzercomputersystem **190** beispielsweise eine Kommunikationsschnittstelle **197** zur Kommunikation mit der Banknote **100** sowie eine Kommunikationsschnittstelle **198** zur Kommunikation über das Netzwerk **160**. Beispielsweise umfasst das Nutzercomputersystem **190** einen Sensor, wie etwa eine Kamera, zum Erfassen von visuellen Angaben **107** der Banknote **100**, wie etwa der Seriennummer **106** der Banknote **100**. Das Nutzercomputersystem **190** ist beispielsweise dazu konfiguriert eine Zahlungsanfrage, etwa von dem Server **170** oder dem Zahlungsdienstserver **200**, an die Banknote **100** und eine Zahlungsautorisierung der Banknote **100** mit einem zahlungsindividuellen Kryptogramm an den Server **170** oder den Zahlungsdienstserver **200** weiterzuleiten. Beispielsweise kann das Nutzercomputersystem **190** dazu konfiguriert sein, direkt oder unter Vermittlung eines Servers wie etwa dem Server **170** oder dem Zahlungsdienstserver **200** den aktuellen Nominalwert der Banknote **100** gemäß dem der Banknote **100** zugeordneten Banknotenkonto zu ermitteln und einem Nutzer unter Verwendung einer Nutzerschnittstelle **191** anzuzeigen. Die Nutzerschnittstelle **191** umfasst beispielsweise eine Eingabe- und eine Ausgabevorrichtung zur Kommunikation des Nutzers mit dem mobilen Kommunikationsgerät **190**. Die Eingabevorrichtung umfasst beispielsweise eine Tastatur und/oder Maus. Die Ausgabevorrichtung umfasst beispielsweise ein Display. Beispielsweise sind Eingabe- und Ausgabevorrichtung in Form eines Touch-Displays miteinander kombiniert.

[0181] Der Server **200** des Zahlungsdienstanbieters ist beispielsweise dazu konfiguriert eine Zahlungsabwicklung unter Verwendung der Banknote **100** und einem lokalen Gerät zur Kommunikation mit der Banknote **100**, wie etwa dem Terminal **130**, mobilen Kommunikationsgerät **180** oder dem Nutzercomputersystem **190**, zu ermöglichen. Der Zahlungsdienstserver **200** umfasst beispielsweise einen Speicher **202**, einen Prozessor **204** zum Ausführen von Programminstruktionen **206** und eine Kommunikationsschnittstelle **208** zur Kommunikation über das Netzwerk **160**. Beispielsweise stellt der Zahlungsdienstserver **200** dem lokalen Gerät Transaktionsdaten einer auszuführenden Transaktion, wie etwa einen Identifikator eines Empfängerkontos und/oder Angaben zu dem zu zahlenden Betrag zur Verfügung. Beispielsweise leitet der Zahlungsdienstserver **200** über das lokale Gerät empfangene Zahlungsautorisierungen an den Zentralbankserver **220** weiter. Beispielsweise leitet der Zahlungsdienstserver **200** von dem Zentralbankserver **220** empfangene Zahlungsbestätigungen an das lokale Gerät weiter.

[0182] Das System umfasst beispielsweise ferner einen Herstellercomputersystem **210**, welches im Zuge der Herstellung der Banknote **100** zum Einsatz kommt. Das Herstellercomputersystem **210** umfasst beispielsweise einen Speicher **212** und einen Prozessor **214** zum Ausführen von Programminstruktionen **216**. Ferner umfasst das Herstellercomputersystem **210** beispielsweise eine Kommunikationsschnittstelle 221 zur Kommunikation mit der Banknote **100**. Beispielsweise sendet das Herstellercomputersystem **210** im Zuge der Initialisierung der der Banknote von dem Zentralbankserver **220** empfangene banknotenindividuelle Daten unter Verwendung der Kommunikationsschnittstelle **217** zur Speicherung an die Banknote **100**, wie etwa die Identifikationsnummer **116** oder den kryptographischen Schlüssel **118**. Ferner umfasst das Herstellercomputersystem **210** beispielsweise einen Sensor **219** zum Prüfen der Banknote **100**. Unter Verwendung des Sensor **219** wird beispielsweise eine Qualitätskontrolle der Banknote **100** durchgeführt. Besteht die Banknote **100** die Qualitätskontrolle wird beispielsweise eine Herstellungsbestätigung von dem Herstellercomputersystem **210** unter Verwendung einer Kommunikationsschnittstelle **218** zur Kommunikation mit einem Computersystem der Zentralbank, wie etwa den Zentralbankserver **220**, an die Zentralbank gesendet. Die Herstellungsbestätigung umfasst beispielsweise die Seriennummer **106** und/oder zur Initialisierung der Banknote **100** dem Zentralbanksystem **156** und zum Einrich-

ten eines Banknotenkontos für die hergestellte Banknote 100

[0183] Fig. 3 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Ausstellen von Banknoten **100**. In Schritt 300 sendet die Zentralbank **220** einen Auftrag zur Herstellung von Banknoten **100** an einen Hersteller **210**, z.B. einer Druckerei. Der Auftrag gibt beispielsweise einen Bereich von Seriennummern vor. Der Bereich von Seriennummern gibt Seriennummern vor, welche für die herzustellenden Banknoten **100** zu verwenden sind. Beispielsweise gibt der Auftrag ferner initiale Nominalwerte für die herzustellenden Banknoten **100** vor. Beispielsweise gibt der Auftrag einen Mindestnominalwert und/oder einen variablen Zusatznominalwertanteil vor. In Schritt 302 stellt der Hersteller **210** die Banknoten **100** gemäß dem empfangenen Auftrag her. Die hergestellten Banknoten **100** umfassen beispielsweise jeweils ein Sicherheitselement mit einem Prozessor. Ferner umfassen die hergestellten Banknoten **100** beispielsweise jeweils eine visuelle Angabe einer der Seriennummern aus dem vorgegebenen Bereich von Seriennummern, welche der jeweiligen Banknote im Zuge des Herstellungsprozesses zugeordnet wurde. In Schritt 304 liest der Hersteller **210** jeweils die visuelle Angabe der Seriennummern der hergestellten Banknoten **100**. Beispielsweise sind in den Speichern der Banknoten **100** zusätzlich die Seriennummern der Banknoten **100** gespeichert. Beispielsweise liest der Hersteller **210** zusätzlich jeweils die Seriennummer aus den Speichern der Banknoten **100** aus. Ferner umfassen die hergestellten Banknoten **100** beispielsweise jeweils visuelle Angaben eines initialen Nominalwerts und/oder eines Mindestnominalwerts. Beispielsweise liest der Hersteller **210** jeweils die visuellen Angaben des initialen Nominalwertes und/oder des Mindestnominalwerts der hergestellten Banknoten **100**. Beispielsweise sind in den Speichern der Banknoten **100** zusätzlich die initialen Nominalwerte, Mindestnominalwerte und/oder variablen Zusatznominalwertanteile, welche den entsprechenden Banknoten **100** zugeordnet sind, gespeichert. Beispielsweise liest der Hersteller **210** zusätzlich jeweils den initialen Nominalwert, Mindestnominalwert und/oder variablen Zusatznominalwertanteil aus den Speichern der Banknoten **100** aus. In Schritt 306 wird eine Herstellungsbestätigung an die Zentralbank **220** gesendet, welche die hergestellten Banknoten **100** identifiziert. Beispielsweise gibt die Herstellungsbestätigung die Seriennummern der hergestellten Banknoten **100** an. Beispielsweise gibt die Herstellungsbestätigung die initialen Nominalwerte der hergestellten Banknoten **100** an. Beispielsweise gibt die Herstellungsbestätigung Mindestnominalwerte und/oder variable Zusatznominalwertanteile der initialen Nominalwerte an.

[0184] In Schritt 308 speichert die Zentralbank **220** die Seriennummern der hergestellten Banknoten in einem ersten Register bzw. Datenbank **148**. Beispielsweise speichert die Zentralbank ferner für die hergestellten Banknoten **100** jeweils den zugeordneten Nominalwert, Mindestnominalwert und/oder variable Zusatznominalwertanteil des initialen Nominalwerts. In Schritt 310 erzeugt das erste Register **148** bzw. das das erste Register **148** verwaltende Zentralbanksystem **156** für jede der hergestellten Banknoten **100**, deren Seriennummern in dem ersten Register **148** gespeichert werden jeweils eine Identifikationsnummer, welche ein der Zentralbank **220** verwaltetes und der entsprechenden Banknote **100** individuell zugeordnetes anonymes Banknotenkonto identifiziert. Bei der Identifikationsnummer handelt es sich mithin um eine „banknote account number“ (BAN). Die Seriennummer wird beispielsweise zum Identifizieren der Banknote verwendet, die Identifikationsnummer wird beispielsweise zum Identifizieren des Banknotenkonto für eine Zahlungsabwicklung verwendet. Beispielsweise wird die Seriennummer jeweils als ein Seed zu erzeugen der Identifikationsnummer für die entsprechende Banknote verwendet. Beispielsweise wird ferner ein Seed der Zentralbank **220** zum Erzeugen der Identifikationsnummer verwendet. Bei dem Seed der Zentralbank handelt es sich beispielsweise um ein Geheimnis der Zentralbank **220**, wie etwa eine Zufallszahl, ein symmetrischer kryptographischer Schlüssel oder ein privater kryptographischer Schlüssel. Ferner erzeugt das erste Register **148** bzw. das das erste Register **148** verwaltende Zentralbanksystem **156** für jede der hergestellten Banknoten **100** jeweils einen banknotenindividuellen kryptographischen Schlüssel. Bei diesem banknotenindividuellen kryptographischen Schlüssels handelt es sich beispielsweise um einen banknotenindividuellen symmetrischen kryptographischen Schlüssel oder um einen privaten kryptographischen Schlüssel eines banknotenindividuellen asymmetrischen Schlüsselpaars. Die BAN sowie der banknotenindividuelle werden von dem ersten Register **148** intern an einen Server der Zentralbank **220** weitergeleitet.

[0185] In Schritt 312 wird ein erster kryptographisch gesicherter Kanal zwischen einem Server der Zentralbank **220** und einem Computersystem des Herstellers **210** aufgebaut. Über diesen ersten kryptographisch gesicherten Kanal wird die BAN von der Zentralbank **220** an den Hersteller **210** gesendet. Bei dem ersten kryptographisch gesicherten Kanal handelt es beispielsweise um einen Ende-zu-Ende-verschlüsselte Kommunikationsverbindung zwischen der Zentralbank **220** und dem Hersteller **210**. Verschlüsselt ist die Verbindung beispielsweise mit einem ersten symmetrischen Sitzungsschlüssel. In Schritt 314 wird ein zweiter kryptographisch gesicherter Kanal zwischen dem Server der Zentralbank **220** und dem Computersystem des Herstellers **210** aufgebaut. Über diesen zweiten kryptographisch gesicherten Kanal wird der banknotenindividuelle kryptographische Schlüssel der Banknote von

der Zentralbank **220** an den Hersteller **210** gesendet. Bei dem zweiten kryptographisch gesicherten Kanal handelt es beispielsweise um einen Ende-zu-Ende-verschlüsselte Kommunikationsverbindung zwischen der Zentralbank **220** und dem Hersteller **210**. Verschlüsselt ist die Verbindung beispielsweise mit einem zweiten symmetrischen Sitzungsschlüssel.

[0186] In Schritt 316 speichert der Hersteller **210** die BAN und den banknotenindividuellen kryptographischen Schlüssel in einem Speicher des Sicherheitselements der jeweiligen Banknote. Dabei wird der banknotenindividuelle kryptographische Schlüssel beispielsweise in eine geschützten Speicherbereich des Speichers des Sicherheitselements. Ferner registriert das erste Register **148** in Schritt 318 die die Seriennummern der hergestellten Banknoten in einem zweiten Register bzw. Datenbank **150**. Beispielsweise speichert die Zentralbank ferner für die hergestellten Banknoten **100** jeweils den zugeordneten Nominalwert, Mindestnominalwert und/oder variable Zusatznominalwertanteil des initialen Nominalwerts in dem zweiten Register **150**. Dabei dient die Seriennummer beispielsweise als Datenbankzugriffsschlüssel zum Zugreifen auf die in dem zweiten Register **150** gespeicherten Angaben zum Nominalwert der entsprechenden Banknote. Bei dem zweiten Register handelt es sich beispielsweise um ein öffentlich zugängliches Register, welches beispielsweise als Lookup-Tabellen (LUT) bzw. Umsetzungstabellen konfiguriert sein. Das zweite Register erlaubtes beispielsweise jedermann mit der Seriennummer einer Banknote den aktuellen Nominalwert der entsprechenden Banknote, etwa über das Internet, nachzuschlagen.

[0187] **Fig. 4** zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Zahlungsabwicklung mit einem Terminal eines PoS („Point of Sale“) 164. In Schritt 320 stellt der Nutzer **162** eine Banknote **100** für eine bargeldlose Zahlung bereit. In Schritt 322 erstellt der PoS 164 eine Zahlungsanfrage zur Zahlung eines bestimmten Betrags und sendet die Zahlungsanfrage an die Banknote **100**. In Schritt 324 erzeugt die Banknote **100** bzw. das Sicherheitselement der Banknote **100** ein zahlungsindividuelles Kryptogramm zur Autorisierung der Zahlung. Das Kryptogramms wird beispielsweise aus der Identifikationsnummer der Banknote und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt. Der zahlungsindividuelle Code umfasst beispielsweise eine Zeitstempel. Ferner kann der zahlungsindividuelle Code bzw. das Kryptogramm als weitere Eingangswerte den zu zahlenden Betrag und eine Identifikationsnummer eines Kontos des Zahlungsempfängers, auf welchen der Betrag gezahlt werden soll. Beispielsweise wird zur Erzeugung des Kryptogramms auf die Eingangswerte eine Hashunktion oder eine andere Einwegfunktion angewendet und das Ergebnis mit dem banknotenindividuellen kryptographischen Schlüssel verschlüsselt. Alternativ könnten die Eingangswerte auch ohne Anwendung einer Einwegfunktion mit dem banknotenindividuellen kryptographischen Schlüssel verschlüsselt werden. Die Banknote **100** sendet eine das zahlungsindividuelle Kryptogramm umfassende Zahlungsautorisierung an den PoS 164. Die Zahlungsautorisierung umfasst neben dem Kryptogramm beispielsweise die zur Erstellung des Kryptogramms verwendeten Eingangswerte in verschlüsselter Form oder in Klartext, d.h. in unverschlüsselter Form. In Schritt 326 sendet der PoS 164 eine Autorisierungsanfrage zum Validieren der Zahlungsautorisierung der Banknote **100** an das Zentralbanksystem **156**. In Schritt 328 extrahiert das Zentralbanksystem **156** die BAN aus der Zahlungsautorisierung. Falls die Zahlungsautorisierung die BAN in verschlüsselter Form umfasst entschlüsselt das Zentralbanksystem **156** beispielsweise die BAN. Hierzu verfügt das Zentralbanksystem **156** im Falle eines symmetrischen banknotenindividuellen kryptographischen Schlüssels beispielsweise über symmetrischen den banknotenindividuellen kryptographischen Schlüssel. Im Falle eines privaten kryptographischen Schlüssel eines banknotenindividuellen asymmetrischen Schlüsselpaars verfügt das Zentralbanksystem **156** beispielsweise über eine zugehörigen öffentlichen kryptographischen Schlüssel des banknotenindividuellen asymmetrischen Schlüsselpaars.

[0188] Das Zentralbanksystem **156** sendet die BAN an das erste Register **148** zum Validieren, dass es sich bei der BAN um eine gültige in dem ersten Register **148** eingetragene BAN eines existierenden Banknotenkontos der Banknote handelt. Ferner wird das Kryptogramm auf seien Validität geprüft, d.h. es wird geprüft, ob es mit dem banknotenindividuellen kryptographischen Schlüssel der zu der BAN gehörenden Banknote **100** verschlüsselt wurde. Beispielsweise umfasst das erste Register **148** hierzu neben der BAN einen Prüfschlüssel zum Prüfen des banknotenindividuellen kryptographischen Schlüssels. Bei dem Prüfschlüssel handelt es sich beispielsweise um einen symmetrischen oder öffentlichen kryptographischen Schlüssel zum Entschlüsseln von Verschlüsselungen, welche mit dem banknotenindividuellen kryptographischen Schlüssel erstellt wurden. In Schritt 330 bestätigt das erste Register **148**, falls es sich um eine gültige BAN handelt die BAN, und stellt die der BAN zugehörige Seriennummer der entsprechenden Banknote **100** zur Verfügung. Die Seriennummer wird verwendet, um in dem zweiten Register **150** den aktuellen Nominalwert der Banknote nachzuschlagen. Fall der in dem zweiten Register **150** gespeicherte aktuelle Nominalwert der Banknote **100**, bei welchem es sich um das Guthaben auf dem Banknotenkonto der Banknote **100** handelt, ausreichend für die Zahlung ist, erfolgt in Schritt 332 die Zah-

lung. Dazu transferiert die Zentralbank den zu zahlenden Betrag von dem Banknotenkonto der Banknote **100** an ein, beispielsweise in der Zahlungsautorisierung identifiziertes Empfängerkonto. Ferner wird der aktuelle Nominalwert in dem zweiten Register **150** aktualisiert, d.h. um den gezahlten Betrag reduziert. Bei diesem aktualisierten Nominalwert der Banknote handelt es sich beispielsweise um den aktualisierten Kontostand bzw. das aktualisierte Guthaben auf dem Banknotenkonto der Banknote **100**. In Schritt 334 sendet das Zentralbanksystem **156** eine Zahlungsbestätigung an den PoS 164. Die Zahlungsbestätigung umfasst beispielsweise den aktualisierten Nominalwert der Banknote **100**. Ferner ist die Zahlungsbestätigung beispielsweise mit einem Signaturschlüssel des Zentralbanksystems **156** signiert. In Schritt 336 wird die Zahlungsbestätigung von dem PoS beispielsweise an die Banknote **100** weitergeleitet. Die Banknote **100** prüft beispielsweise die Signatur des Zentralbanksystems **156** bzw. der Zentralbank **220** mit einem Signaturprüfschlüssel. Der Signaturprüfschlüssel zum Prüfen von Signatur des Zentralbanksystems **156** bzw. der Zentralbank **220** wird beispielsweise bei der Herstellung in der Banknote **100** bzw. in dem Speicher des Sicherheitselements der Banknote **100** hinterlegt. Bei dem Signaturschlüssel handelt es sich beispielsweise um einen privaten kryptographischen Schlüssel eines asymmetrischen Schlüsselpaars des Zentralbanksystems **156**, während des sich bei dem Signaturprüfschlüssel beispielsweise um einen öffentlichen kryptographischen Schlüssel des entsprechenden asymmetrischen Schlüsselpaars handelt. Falls die Signaturprüfung erfolgreich ist, ersetzt die Banknote **100** den in dem Speicher des Sicherheitselements gespeicherten Nominalwert beispielsweise durch den aktualisierten Nominalwert gemäß der Zahlungsbestätigung des Zentralbanksystems **156**.

[0189] Fig. 5 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Bestätigung eines aktuellen Nominalwerts **109** einer Banknote **100**. In Schritt 340 stellt der Nutzer **162** eine Banknote **100** einem mobilen tragbaren Kommunikationsgerät **180**, z.B. einem Smartphone, zum Ermitteln des aktuellen Nominalwerts der entsprechenden Banknote **100** bereit. Beispielsweise verwendet der Nutzer hierzu eine auf dem mobilen Kommunikationsgerät **180** installierte App, in welcher er eine Verifikation des in der Bankknote gespeicherten Nominalwerts anfragt. In Schritt 342 sendet das mobile Kommunikationsgerät **180** daraufhin eine Ausgabeanfrage zum Ausgeben des in dem Speicher des Sicherheitselements der Banknote **100** gespeicherten aktuellen Nominalwerts sowie beispielsweise der Seriennummer der Banknote als Identifikator der Banknote **100**. In Schritt 344 sendet die Banknote **100** in Antwort den gespeicherten Nominalwert NW(BN) und die Seriennummer der Banknote **100** an das mobile Kommunikationsgerät **180**. Die Seriennummer kann auch unter Verwendung der visuellen Angabe derselben mit einem optischen Sensor des mobilen Kommunikationsgerät **180**, wie etwa einer Kamera erfasst werden. In Schritt 346 sendet das mobile Kommunikationsgerät **180** ferner eine Anfrage nach dem in dem zweite Register **150** für die Seriennummer der Banknote **100** gespeicherten aktuellen Nominalwert an das Zentralbanksystem **156**. In Schritt 348 empfängt das mobilen Kommunikationsgerät **180** in Antwort den in dem zweiten Register **150** für die Banknote **100** gespeicherten aktuellen Nominalwert NW(R2). In Schritt 350 vergleicht das mobile Kommunikationsgerät **180** die beiden Nominalwerte NW(BN) und NW (R2) miteinander. Falls diese beide Werte übereinstimmen, bestätigt das mobile Kommunikationsgerät **180** den in der Banknote **100** gespeicherten Nominalwert als aktuell und zeigt diesen beispielsweise auf einer Anzeigevorrichtung, wie etwa einem Display, für den Nutzer **162** an. Falls die beiden Werte nicht übereinstimmen, leitet das mobile Kommunikationsgerät **180** den in dem zweiten Register **150** gespeicherten aktuellen Nominalwert NW(R2) beispielsweise an die Banknote **100** zum Aktualisieren des dort gespeicherten Nominalwerts weiter. Zum Nachweis der Authentizität des Nominalwert NW(R2) ist dieser von dem Zentralbanksystem **156** beispielsweise mit einem Signaturschlüssel signiert.

[0190] Fig. 6 zeigt ein schematisches Blockdiagramm exemplarischer Verfahren zum Verwenden von Banknoten **100**. Die Zentralbank **220** gibt die Banknoten **100** aus. Die Zentralbank **220** erzeugt in Zuge der Initialisierung der Banknoten **100** eine Identifikationsnummer für die Banknote **100**, welche ein von der Zentralbank verwaltetes und der entsprechenden Banknote **100** individuell zugeordnetes anonymes Banknotenkonto identifiziert. Ferner erzeugt die Zentralbank beispielsweise einen banknotenindividuellen kryptographischen Schlüssel für die Banknoten **100**. Identifikationsnummer und kryptographischer Schlüssel werden der Banknote **100** beispielsweise von der Zentralbank **220** bereitgestellt und in dem Sicherheitselement der Banknote **100** gespeichert. Beispielsweise kann der einen banknotenindividuellen kryptographischen Schlüssel auch von der Banknote **100** selbst erzeugt werden, etwa als privater kryptographischer Schlüssel eines asymmetrischen Schlüsselpaars der der Banknote **100**. In diesem Fall kann der Zentralbank **220** beispielsweise ein zugehöriger öffentlicher kryptographischer Schlüssel des asymmetrischen Schlüsselpaars als Prüfschlüssel zum Prüfen von Kryptogrammen der Banknote zur Verfügung gestellt werden. Dem von der Identifikationsnummer identifizierten Banknotenkonto der Banknote **100** wird ein initialer Nominalwert der Banknote **100** als Guthaben gutgeschrieben. Dies erfolgt beispielsweise durch die Zentralbank. Die initialen Nominalwerte werden beispielsweise von der Zentralbank bei der Herstellung der Banknoten **100** vorgegeben. Die Gutschrift der initialen Nominalwerte auf den

Banknotenkonten bzw. die Initialisierung der Banknoten erfolgt beispielsweise auf ein Erzeugen der zugehörigen Identifikationsnummer durch die Zentralbank hin. Die Identifikationsnummern werden beispielsweise jeweils für eine bestimmte Seriennummer einer hergestellten Banknote erzeugt. Die Identifikationsnummer, Seriennummern und/oder banknotenindividuellen Prüfschlüssel zum Prüfen von Kryptogrammen der entsprechenden Banknoten werden in einem ersten von der Zentralbank **220** verwalteten Register **148** gespeichert. In einem zweiten der Zentralbank **220** verwalteten Register **150** werden die aktuellen Nominalwerte, d.h. die aktuellen Guthaben der Banknotenkonten, gespeichert. Die Zuordnung zu den Banknoten **100** erfolgt beispielsweise anhand der Seriennummern der Banknoten **100**, welche als Datenbankzugriffsschlüssel für das zweite Register **150** dienen.

[0191] Sind die Banknoten **100** hergestellt gelangen sie in den freien Zahlungsverkehr **165**. Sie können als Barzahlungsmittel von einem Nutzer **162** an eine Zahlungsempfänger **161** übergebe werden. Mit der Übergabe geht nicht nur das Eigentum an der Banknote **100**, sondern auch an dem der Banknote **100** zugeordneten Guthaben auf dem Banknotenkonto, d.h. dem aktuellen Nominalwert der Banknote, an den Zahlungsempfänger **161** über. Ferner kann der Nutzer **162** die Banknote **100** zur Zahlung mittels eines mobilen tragbaren Kommunikationsgeräts **180**, wie etwa einem Smartphone, verwenden. Beispielsweise können Zahlungen über das Internet abgewickelt werden, bei welchen das mobile Kommunikationsgerät **180** als lokales Terminal fungiert. Beispielsweise können Zahlungen von dem Banknotenkonto auf andere Konten gesendet bzw. veranlasst werden. Beispielsweise können Zahlungen von dem Banknotenkonto auf andere Banknotenkonten gesendet bzw. veranlasst werden. Ferner können mittels des mobile Kommunikationsgerät **180** beispielsweise die Banknote **100** und/oder ein auf der Banknote gespeicherter aktueller Nominalwert verifiziert werden. Schließlich kann die Banknote **100** beispielsweise zum Zahlen an einem Terminal **130**, beispielsweise eines PoS, verwendet werden. Zur Autorisierung einer Zahlung erzeugt die Banknote **100** ein zahlungsindividuelles Kryptogramm unter Verwendung des banknotenindividuellen kryptographischen Schlüssels. Das Terminal kann beispielsweise mit einem Zahlungsdienstleister **200** (engl. „Payment-Service-Provider“/PSP) kommunizieren, welcher beispielsweise die Zahlungsabwicklung unter Verwendung des Kryptogramms vornimmt. Der Zahlungsdienstleister **200** leitet das Kryptogramm zur Zahlungsabwicklung beispielsweise an die Zentralbank **220** weiter, welche das Kryptogramm unter Verwendung des ersten Registers **148** prüft. Ist das Kryptogramm valide und der Nominalwert der Banknote **100** gemäß dem zweiten Register **150** ausreichend für die Zahlung verbucht die Zentralbank **220** die Zahlung und bestätigt diese gegenüber dem Zahlungsdienstleister **200**. Die Zahlungsbestätigung wird beispielsweise von dem Zahlungsdienstleiser **200** über das Terminal **130** an die Banknote **100** weitergeleitet. Die Zahlungsbestätigung umfasst beispielsweise den aus der Zahlung resultierenden aktuellen Nominalwert der Banknote **100**. Die Banknote **100** kann unter Verwendung des von der Zahlungsbestätigung bereitgestellten aktuellen Nominalwert den in der Banknote **100** gespeicherten bisherigen Nominalwert aktualisieren. Maßgeblich für den tatsächlichen Nominalwert einer Banknote **100** ist im vorliegenden Fall beispielsweise der Kontostand bzw. das Guthaben des Banknotenkontos der Banknote **100**.

[0192] Fig. 7 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Verwenden einer Banknote. Die Banknote umfasst eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer eines initialen Nominalwerts der Banknote. Die Banknote umfasst ein Sicherheitselement mit einem Prozessor und einem Speicher. In dem Speicher des Sicherheitselements ist eine Identifikationsnummer der Banknote gespeichert, welche ein von einer die Banknote ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote individuell zugeordnetes anonymes Banknotenkonto identifiziert. In einem geschützten Speicherbereich des Speichers des Sicherheitselements ist ferner ein banknotenindividueller kryptographischer Schlüssel gespeichert.

[0193] In Block 600 wird eine Zahlungsanfrage für eine Zahlung mit der Banknote empfangen. In Block 602 wird ein zahlungsindividuelles Kryptogramm zur Autorisierung der Zahlung mit der Banknote erzeugt. Die Identifikationsnummer der Banknote und ein zahlungsindividueller Code dienen dabei als Eingangswerte, aus welchen unter Verwendung des banknotenindividuellen kryptographischen Schlüssels das Kryptogramm erzeugt wird. Block 604 wird eine das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung gesendet.

[0194] Fig. 8 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Aktualisieren eines Nominalwerts einer Banknote. In Block 610 empfängt die Banknote eine Aktualisierungsanfrage zum Aktualisieren eines aktuellen Nominalwerts der Banknote, welcher in einem Speicher eines Sicherheitselements der Banknote gespeicherte ist. Die Aktualisierungsanfrage umfasst einen aktualisierten Nominalwert der Banknote zusammen mit einer kryptographisch gesicherten Bestätigung der Zentralbank für den aktualisierten Nominalwert. In Block 612 prüft die Banknote die Aktualisierungsanfrage. In Block 614 ermittelt die Banknote im Zuge des Prüfens der Aktualisierungsanfrage, ob die kryptographisch gesicherte Bestätigung valide ist. Hierzu verwendet die Banknote einen in dem Speicher des Si-

cherheitselements gespeicherten kryptographischen Prüfschlüssel. Falls eine entsprechende Bestätigung fehlt oder invalide ist, wird das Verfahren in Block 616 abgebrochen. Falls die entsprechende Bestätigung valide ist, wird in Block 618 der in dem Speicher des Sicherheitselements gespeicherte aktuelle Nominalwert der Banknote mit dem empfangenen aktualisierten Nominalwert ersetzt.

[0195] Fig. 9 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Ausgeben eines Nominalwerts einer Banknote. In Block 620 empfängt die Banknote eine Ausgabeanfrage zum Ausgeben des in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote. In Antwort auf die Anfrage, sendet die Banknote in Block 622 den in dem Speicher des Sicherheitselements gespeicherten aktuellen Nominalwerts der Banknote.

[0196] Fig. 10 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zum Ausstellen einer Banknote. In Block 630 wird die Banknote hergestellt, Die hergestellte Banknote umfasst eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer der Banknote aus einem vordefinierten Bereich von Seriennummern sowie einen der Banknote zugeordneten initialen Nominalwert. Ferner umfasst die Banknote ein Sicherheitselement mit einem Prozessor und einem Speicher mit Programminstruktionen. In Block 632 wird eine Identifikationsnummer der Banknote über einen ersten kryptographisch gesicherten Kanal empfangen. Diese Identifikationsnummer identifiziert ein von einer die Banknote ausgebenden Zentralbank verwaltetes und der entsprechenden Banknote individuell zugeordnetes anonymes Banknotenkonto. In Block 634 wird die empfangenen Identifikationsnummer in dem Speicher des Sicherheitselements gespeichert. In Block 636 wird ein banknotenindividueller kryptographischer Schlüssel über einen von dem ersten Kanal unabhängigen zweiten kryptographisch gesicherten Kanal empfangen. In Block 638 wird der empfangene banknotenindividuelle kryptographische Schlüssel in einem geschütz-ten Speicherbereich des Speichers des Sicherheitselements gespeichert. In Block 640 wird der initiale Nominalwert der Banknote als aktuellen Nominalwert in dem Speicher des Sicherheitselements gespeichert. In Block 642 wird die Seriennummer der Banknote in dem Speicher des Sicherheitselements gespeichert. In Block 644 wird ein öffentlicher kryptographischer Schlüssel eines asymmetrischen Schlüsselpaars der ausgebenden Zentralbank in dem Speicher der Banknote gespeichert.

[0197] Fig. 11 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Zahlungsabwicklung mit einem Terminal. Diese Zahlung erfolgt mit einer Banknote, welche eine visuelle Angabe einer die Banknote eindeutig identifizierenden Seriennummer der Banknote und eines der Banknote zugeordneten initialen Nominalwerts umfasst. Ferner umfasst die Banknote eine Kommunikationsschnittstelle zur Kommunikation mit dem Terminal und ein Sicherheitselement mit einem Prozessor und einem Speicher umfasst. In dem Speicher des Sicherheitselements ist eine Identifikationsnummer der Banknote gespeichert. Diese Identifikationsnummer identifiziert ein anonymes Banknotenkonto, welches von einer die Banknote ausgebenden Zentralbank verwaltet wird und der entsprechenden Banknote individuell zugeordnet ist. In einem geschützten Speicherbereich des Speichers des Sicherheitselements ist ein banknotenindividueller kryptographischer Schlüssel gespeichert. Das Terminal umfasst einen Prozessor, einen Speicher und eine Kommunikationsschnittstelle zur Kommunikation mit der Banknote.

[0198] In Block 650 sendet das Terminal eine Zahlungsanfrage an die Banknote. In Block 650 empfängt das Terminal ein zahlungsindividuelles Kryptogramm zur Autorisierung der Zahlung mit der Banknote. Das Kryptogramm ist aus der Identifikationsnummer der Banknote und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels erzeugt. In Block 654 leitet das Terminal das zahlungsindividuelle Kryptogramm mit einer Angabe des zu zahlenden Betrags an die ausgebende Zentralbank weiter für eine Validierung des zahlungsindividuellen Kryptogramms. Ferner ist prüft die Zentralbank in einem Register, ob der aktuelle Nominalwert der Banknote größer oder gleich dem zu zahlenden Betrag ist. Fallen alle Prüfungen seitens der Zentralbank positiv aus, wir der Zahlungstransfer ausgeführt. Falls der Zahlungstransfer auf eine erfolgreiche Validierung und Registerprüfung durch die Zentralbank erfolgreich ausgeführt ist, empfängt das Terminal Block 656 eine Bestätigung über den erfolgreichen Zahlungstransfer.

[0199] Fig. 12 zeigt ein schematisches Flussdiagramm eines exemplarischen Verfahrens zur Zahlungsabwicklung mit einer Mehrzahl von Banknoten. In Block 660 wird eine Mehrzahl von Banknoten empfangen. In Block 662 wird für jede der Banknoten jeweils ein aktueller Nominalwert ermittelt. In Block 664 wird aus der Mehrzahl von empfangenen Banknoten ein Satz von Banknoten ausgewählt und einbehalten, deren aufsummierte aktuelle Nominalwerte einen Betrag ergeben, der kleiner als ein zu zahlender Betrag ist. In Block 666 wird eine Zahlungsanfrage zur Zahlung eines verbleibenden Differenzbetrags an eine weitere Banknote der Mehrzahl von Banknoten gesendet, welche nicht von dem Satz von ausgewählten Banknoten umfasst ist. Der verbleibende Differenzbetrag zwischen dem zu zahlenden Betrag und dem aufsummierten Betrag des Satzes von ausgewählten Banknoten ist dabei kleiner als ein aktueller Nominalwert der weiteren Banknote.

Bezugszeichenliste

100 Banknote
102 Sicherheitselement
104 Kommunikationsschnittstelle
106 Seriennummer
107 visuelle Angabe
108 initialer Nominalwert
109 aktueller Nominalwert
110 Sicherheitsmerkmal
112 Nutzerschnittstelle
116 Identifikationsnummer
118 kryptographischer Schlüssel
120 Speicher
122 geschützter Speicherbereich
124 Prozessor
128 Programminstruktionen
130 Terminal
132 Speicher
134 Prozessor
136 Programminstruktionen
137 Kommunikationsschnittstelle
138 Kommunikationsschnittstelle
139 Sensor
148 Register 1
150 Register 2
156 Zentralbanksystem
160 Netzwerk
162 Nutzer
161 Zahlungsempfänger
164 PoS
165 Zahlungsverkehr
170 Server
172 Speicher
174 Prozessor
176 Programminstruktionen
178 Kommunikationsschnittstelle
180 mobiles tragbares Kommunikationsgerät
181 Nutzerschnittstelle
182 Speicher
184 Prozessor
186 Programminstruktionen
187 Kommunikationsschnittstelle
188 Kommunikationsschnittstelle
189 Kamera
190 Nutzercomputersystem
191 Nutzerschnittstelle
192 Speicher
194 Prozessor
196 Programminstruktionen
197 Kommunikationsschnittstelle
198 Kommunikationsschnittstelle
199 Sensor
200 Zahlungsdienstserver
202 Speicher
204 Prozessor
206 Programminstruktionen
208 Kommunikationsschnittstelle
210 Herstellercomputersystem
212 Speicher
214 Prozessor
216 Programminstruktionen
217 Kommunikationsschnittstelle
218 Kommunikationsschnittstelle
219 Sensor
220 Zentralcomputersystem
222 Speicher
224 Prozessor
226 Programminstruktionen
228 Kommunikationsschnittstelle
229 Sensor

Patentansprüche

1. Banknote (100) umfassend ein Sicherheitselement (102) mit einem Prozessor (124) und einem Speicher (120) mit Programminstruktionen (128) umfasst,
wobei in dem Speicher (120) des Sicherheitselements (102) eine Identifikationsnummer (116) der Banknote (100) gespeichert ist, welche ein von einer die Banknote (100) ausgebenden Zentralbank (220) verwaltetes und der entsprechenden Banknote (100) individuell zugeordnetes anonymes Banknotenkonto identifiziert, wobei in einem geschützten Speicherbereich (122) des Speichers (120) des Sicherheitsele-

ments (102) ein banknotenindividueller kryptographischer Schlüssel (118) gespeichert ist,
wobei der Prozessor (124) dazu konfiguriert ist bei Ausführen der Programminstruktionen (128) ein Zahlungsverfahren mit der Banknote (100) auszuführen, wobei das Zahlungsverfahren umfasst:
• Empfangen einer Zahlungsanfrage für eine Zahlung mit der Banknote (100),
• Erzeugen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote (100), wobei das Kryptogramm aus der Identifikationsnummer (116) der Banknote (100) und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels (118) erzeugt wird,
• Senden einer das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung.

2. Banknote (100) nach Anspruch 1, wobei die Banknote eine visuelle Angabe (107) eines der Banknote (100) zugeordneten initialen Nominalwerts (108) umfasst.

3. Banknote (100) nach einem der vorangehenden Ansprüche, wobei die Banknote eine visuelle Angabe (107) einer die Banknote (100) eindeutig identifizierenden Seriennummer (106) und/oder der Identifikationsnummer (116) umfasst.

4. Banknote (100) nach einem der vorangehenden Ansprüche, wobei die Banknote (100) eine Mehrzahl von Sicherheitsmerkmalen (110) umfasst, wobei ein oder mehrere Sicherheitsmerkmale (110) der Mehrzahl von Sicherheitsmerkmalen (110) eine Angabe der Seriennummer (106) und/oder der Identifikationsnummer (116) der Banknote (100) umfassen.

5. Banknote (100) nach einem der vorangehenden Ansprüche, wobei es sich bei der Identifikationsnummer (116) um die Seriennummer (106) der Banknote (100) handelt.

6. Banknote (100) nach einem der vorangehenden Ansprüche, wobei es sich bei der Identifikationsnummer um eine Banknotenkontonummer des der Banknote (100) individuell zugeordneten anonymen Banknotenkontos handelt.

7. Banknote (100) nach einem der vorangehenden Ansprüche, wobei die Zahlungsanfrage einen zu zahlenden Betrag angibt und der zu zahlende Betrag als zusätzlicher Eingangswert zum Erzeugen des zahlungsindividuellen Kryptogramms verwendet wird.

8. Banknote (100) nach einem der vorangehenden Ansprüche, wobei die Zahlungsautorisierung ferner die Identifikationsnummer (116) und/oder den zahlungsindividuellen Code in Klartext umfasst.

9. Banknote (100) nach einem der vorangehenden Ansprüche, wobei die Banknote (100) eine Kommunikationsschnittstelle (104) zur Kommunikation mit einem Terminal (130) umfasst, wobei die Banknote (100) die Zahlungsanfrage von dem Terminal (130) über die Kommunikationsschnittstelle (104) empfängt und/oder die Zahlungsautorisierung über die Kommunikationsschnittstelle (104) an das Terminal (130) sendet.

10. Banknote (100) nach einem der vorangehenden Ansprüche, wobei in dem Speicher (120) des Sicherheitselements (102) ferner ein aktueller Nominalwert (109) der Banknote (100) gespeichert ist.

11. Banknote (100) nach Anspruch 10, wobei der Prozessor (124) ferner dazu konfiguriert ist bei Ausführen der Programminstruktionen (128) den zu zahlenden Betrag mit dem gespeicherten aktuellen Nominalwert (109) der Banknote (100) abzugleichen und das zahlungsindividuelle Kryptogramms zur Autorisierung der Zahlung nur unter der Voraussetzung zu erzeugen, dass der gespeicherte aktuelle Nominalwert (109) größer oder gleich dem zu zahlenden Betrag ist.

12. Banknote (100) nach einem der Ansprüche 10 bis 11, wobei der Prozessor (124) ferner dazu konfiguriert ist bei Ausführen der Programminstruktionen (128) ein Aktualisierungsverfahren zum Aktualisieren des gespeicherten aktuellen Nominalwerts (109) der Banknote (100) auszuführen, wobei das Aktualisierungsverfahren umfasst:
• Empfangen einer Aktualisierungsanfrage zum Aktualisieren des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100), wobei die Aktualisierungsanfrage einen aktualisierten Nominalwert der Banknote (100) zusammen mit einer kryptographisch gesicherten Bestätigung der ausgebenden Zentralbank (220) für den aktualisierten Nominalwert umfasst,
• Prüfen der kryptographisch gesicherten Bestätigung unter Verwendung eines in dem Speicher (120) des Sicherheitselements (102) gespeicherten kryptographischen Prüfschlüssels,
• im Falle einer erfolgreichen Prüfung, Ersetzten des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100) mit dem empfangenen aktualisierten Nominalwert.

13. Banknote (100) nach einem der Ansprüche 10 bis 12, wobei der Prozessor (124) ferner dazu konfiguriert ist bei Ausführen der Programminstruktionen (128) ein Ausgabeverfahren zum Ausgeben des gespeicherten aktuellen Nominalwerts (109) der Banknote (100) auszuführen, wobei das Ausgabeverfahren umfasst:

• Empfangen einer Ausgabeanfrage zum Ausgeben des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100),
• in Antwort auf die Ausgabeanfrage, Senden des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100).

14. Banknote (100) nach Anspruch 13, wobei zusammen mit dem gespeicherten aktuellen Nominalwert (109) der Banknote (100) die Seriennummer (106) und/oder die Identifikationsnummer (116) der Banknote (100) gesendet wird und dem Empfänger des aktuellen Nominalwerts als Identifikator der Banknote (100) für eine Bestätigungsanfrage an die Zentralbank (220) zum Bestätigen des empfangenen aktuellen Nominalwerts (109) der Banknote (100) dient.

15. Banknote (100) nach einem der Ansprüche 13 bis 14, wobei die Banknote (100) eine Kommunikationsschnittstelle (104) zur kontaktlosen Kommunikation mit einem mobilen tragbaren Telekommunikationsgerät (180) umfasst, wobei die Banknote (100) die Ausgabeanfrage von dem mobilen tragbaren Telekommunikationsgerät (180) über die Kommunikationsschnittstelle (104) empfängt und/oder den in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100) über die Kommunikationsschnittstelle (104) an das mobile tragbare Telekommunikationsgerät (180) sendet.

16. Banknote (100) nach einem der Ansprüche 13 bis 15, wobei die Banknote (100) eine Nutzerschnittstelle (112) zur Kommunikation mit einem Nutzer (162) der Banknote (100) umfasst, wobei die Banknote (100) die Ausgabeanfrage von einem Nutzer (162) über eine Eingabevorrichtung der Nutzerschnittstelle (112) empfängt und/oder den in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100) an die Nutzerschnittstelle (112) zum Ausgeben über eine Anzeigevorrichtung der Nutzerschnittstelle (112) sendet.

17. Verfahren zum Ausstellen einer Banknote (100), wobei das Verfahren umfasst:
• Herstellen der Banknote (100), wobei die Banknote (100) ein Sicherheitselement (102) mit einem Prozessor (124) und einem Speicher (120) mit Programminstruktionen (128) umfasst,
• Empfang einer Identifikationsnummer (116) der Banknote (100) über einen ersten kryptographisch gesicherten Kanal, wobei die Identifikationsnummer (116) ein von einer die Banknote (100) ausgebenden Zentralbank (220) verwaltetes und der entsprechenden Banknote (100) individuell zugeordnetes anonymes Banknotenkonto identifiziert,
• Speichern der empfangenen Identifikationsnummer (116) in dem Speicher (120) des Sicherheitselements (102),
• Empfang eines banknotenindividuellen kryptographischen Schlüssels (118) über einen von dem ersten Kanal unabhängigen zweiten kryptographisch gesicherten Kanal,
• Speichern des empfangenen banknotenindividuellen kryptographischen Schlüssels (118) in einem geschützten Speicherbereich (122) des Speichers (120) des Sicherheitselements (102).

18. Verfahren zum Ausstellen der Banknote (100) nach Anspruch 17, wobei das Verfahren ferner ein Speichern des initialen Nominalwerts (108) der Banknote (100) als aktuellen Nominalwert (109) in dem Speicher (120) des Sicherheitselements (102) umfasst.

19. Verfahren zum Ausstellen der Banknote (100) nach einem der Ansprüche 17 bis 18, wobei das Verfahren ferner ein Speichern der Seriennummer (106) der Banknote (100) in dem Speicher (120) des Sicherheitselements (102) umfasst.

20. Verfahren zum Ausstellen der Banknote (100) nach einem der Ansprüche 17 bis 19, wobei das Verfahren ferner ein Speichern eines öffentlichen kryptographischen Schlüssels eines asymmetrischen Schlüsselpaars der ausgebenden Zentralbank (220) umfasst.

21. Verfahren zum Ausstellen der Banknote (100) nach einem der Ansprüche 17 bis 20, wobei das Verfahren ferner ein Senden einer Herstellungsbestätigung zu Bestätigung der Herstellung der Banknote (100) an die ausgebende Zentralbank (220) umfasst, wobei die Herstellungsbestätigung die Seriennummer (106) und den initialen Nominalwert (108) der hergestellten Banknote (100) zum Speichern in einem ersten Register (148) der ausgebenden Zentralbank (220) umfasst, wobei der initiale Nominalwert (108) den aktuellen Nominalwert (109) der Banknote (100) bei der Ausstellung angibt, wobei die Identifikationsnummer (116) der Banknote (100) und der banknotenindividuelle kryptographische Schlüssel (118) in Antwort auf das Senden der Herstellungsbestätigung zum Speichern in dem Sicherheitselement (102) empfangen werden.

22. Verfahren zum Ausstellen der Banknote (100) nach Anspruch 21, wobei Identifikationsnummer (116) und der banknotenindividuelle kryptographische Schlüssel (118) in Antwort auf das Senden der Herstellungsbestätigung empfangen werden, nachdem die ausgebende Zentralbank (220) die Identifikationsnummer (116) und/oder den banknotenindividuellen kryptographischen Schlüssel (118) in einem zweiten Register (150) gespeicherte hat, welches die Identifikationsnummer (116) und/oder den

banknotenindividuellen kryptographischen Schlüssel (118) der Seriennummer (106) der Banknote (100) zuordnet.

23. Verfahren zum Verwenden einer Banknote (100), wobei die Banknote (100) ein Sicherheitselement (102) mit einem Prozessor (124) und einem Speicher (120) umfasst,
wobei in dem Speicher (120) des Sicherheitselements (102) eine Identifikationsnummer (116) der Banknote (100) gespeichert ist, welche ein von einer die Banknote (100) ausgebenden Zentralbank (220) verwaltetes und der entsprechenden Banknote (100) individuell zugeordnetes anonymes Banknotenkonto identifiziert, wobei in einem geschützten Speicherbereich (122) des Speichers (120) des Sicherheitselements (102) ein banknotenindividueller kryptographischer Schlüssel (118) gespeichert ist,
wobei das Verfahren zum Zahlen mit der Banknote (100) umfasst:
• Empfangen einer Zahlungsanfrage für eine Zahlung mit der Banknote (100),
• Erzeugen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote (100), wobei das Kryptogramm aus der Identifikationsnummer (116) der Banknote (100) und einem zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels (118) erzeugt wird,
• Senden einer das zahlungsindividuelle Kryptogramm umfassenden Zahlungsautorisierung.

24. Verfahren zum Verwenden der Banknote (100) nach Anspruch 23, wobei die Zahlungsanfrage einen zu zahlenden Betrag angibt, wobei das Verfahren zum Zahlen ferner ein Abgleichen des zu zahlenden Betrags mit einem in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwert (109) der Banknote (100) umfasst und das zahlungsindividuelle Kryptogramm zum Autorisieren der Zahlung nur unter der Voraussetzung erzeugt wird, dass der gespeicherte aktuelle Nominalwert (109) der Banknote (100) größer oder gleich dem zu zahlenden Betrag ist.

25. Verfahren zum Verwenden der Banknote (100) nach Ansprüche 23 bis 24, wobei das Verfahren ferner zum Aktualisieren des gespeicherten aktuellen Nominalwerts (109) der Banknote (100) umfasst:
• Empfangen einer Aktualisierungsanfrage zum Aktualisieren des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100), wobei die Aktualisierungsanfrage einen aktualisierten Nominalwert der Banknote (100) zusammen mit einer kryptographisch gesicherten Bestätigung der Zentralbank (220) für den aktualisierten Nominalwert umfasst,
• Prüfen der kryptographisch gesicherten Bestätigung unter Verwendung eines in dem Speicher des Sicherheitselements (102) gespeicherten kryptographischen Prüfschlüssels,
• im Falle einer erfolgreichen Prüfung, Ersetzten des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100) mit dem empfangenen aktualisierten Nominalwert.

26. Verfahren zum Verwenden der Banknote (100) nach Ansprüche 23 bis 25, wobei das Verfahren ferner zum Ausgeben des gespeicherten aktuellen Nominalwerts (109) der Banknote (100) umfasst:
• Empfangen einer Ausgabeanfrage zum Ausgeben des in dem Speicher des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100),
• in Antwort auf die Anfrage, Senden des in dem Speicher des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100).

27. Verfahren zum Verwenden der Banknote (100) nach Anspruch 26, wobei in dem Speicher (120) des Sicherheitselements (102) ferner die Seriennummer (106) der Banknote (100) gespeichert ist, welche zusammen mit dem gespeicherten aktuellen Nominalwert (109) der Banknote (100) gesendet wird und dem Empfänger des aktuellen Nominalwerts (109) als Identifikator der Banknote (100) für eine Bestätigungsanfrage an die Zentralbank (220) zum Bestätigen des empfangenen aktuellen Nominalwerts (109) der Banknote (100) dient.

28. Verfahren zur Zahlungsabwicklung unter Verwenden eines Terminals (130), wobei die Banknote (100) eine Kommunikationsschnittstelle (104) zur Kommunikation mit dem Terminal (130) und ein Sicherheitselement (102) mit einem Prozessor (124) und einem Speicher (120) umfasst,
wobei in dem Speicher (120) des Sicherheitselements (102) eine Identifikationsnummer (116) der Banknote (100) gespeichert ist, welche ein von einer die Banknote (100) ausgebenden Zentralbank (220) verwaltetes und der entsprechenden Banknote (100) individuell zugeordnetes anonymes Banknotenkonto identifiziert, wobei in einem geschützten Speicherbereich (122) des Speichers (120) des Sicherheitselements (102) ein banknotenindividueller kryptographischer Schlüssel (118) gespeichert ist,
wobei das Terminal (130) einen Prozessor (134), einen Speicher (132) und eine Kommunikationsschnittstelle (137) zu Kommunikation mit der Banknote (100) umfasst
wobei das Verfahren zur Abwicklung eines Zahlungstransfers durch das Terminal (130) umfasst:
• Senden einer Zahlungsanfrage an die Banknote (100),
• Empfangen eines zahlungsindividuellen Kryptogramms zur Autorisierung der Zahlung mit der Banknote (100), wobei das Kryptogramm aus der Identifikationsnummer (116) der Banknote (100) und einem

zahlungsindividuellen Code als Eingangswerte unter Verwendung des banknotenindividuellen kryptographischen Schlüssels (118) erzeugt ist,
• Weiterleiten des zahlungsindividuellen Kryptogramms mit einer Angabe des zu zahlenden Betrags an die ausgebende Zentralbank (220) für eine Validierung des zahlungsindividuellen Kryptogramms, eine Registerprüfung, ob der aktuelle Nominalwert (109) der Banknote (100) größer oder gleich dem zu zahlenden Betrag ist, und einer Ausführung des Zahlungstransfers,
• falls der Zahlungstransfer auf eine erfolgreiche Validierung und Registerprüfung durch die Zentralbank (220) hin erfolgreich ausgeführt ist, Empfangen einer Bestätigung über den erfolgreichen Zahlungstransfer.

29. Verfahren zur Zahlungsabwicklung nach Anspruch 28, wobei mit dem zahlungsindividuellen Kryptogramm ferner die Seriennummer (106) und/oder Identifikationsnummer (116) der Banknote (100) an die ausgebende Zentralbank (220) gesendet werden.

30. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 29, wobei mit dem zahlungsindividuellen Kryptogramm ferner der zahlungsindividuelle Code empfangen und mit dem zahlungsindividuellen Kryptogramm an die ausgebende Zentralbank (220) gesendet wird.

31. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 30, wobei die ausgebende Zentralbank (220) über einen Prüfschlüssel zum Prüfen der Validität des zahlungsindividuellen Kryptogramms verfügt.

32. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 31, wobei ferner eine Identifikationsnummer eines Empfängerkontos zum Empfangen des zu zahlenden Betrags an die ausgebende Zentralbank (220) gesendet wird.

33. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 32, wobei die Bestätigung des Zahlungstransfers kryptographisch gesichert ist und das Verfahren ferner ein Prüfen der Bestätigung unter Verwendung eines kryptographischen Prüfschlüssels umfasst.

34. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 33, wobei die Bestätigung des Zahlungstransfers eine Angabe des aktualisierten Nominalwerts der Banknote (100) zusammen mit einer kryptographisch gesicherten Bestätigung der Zentralbank (220) für den aktualisierten Nominalwert umfasst.

35. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 33, wobei das Verfahren ferner umfasst ein Senden einer Aktualisierungsanfrage zum Aktualisieren des in dem Speicher (120) des Sicherheitselements (102) gespeicherten aktuellen Nominalwerts (109) der Banknote (100), wobei die Aktualisierungsanfrage den aktualisierten Nominalwert der Banknote (100) zusammen mit der kryptographisch gesicherten Bestätigung der Zentralbank (220) für den aktualisierten Nominalwert umfasst.

36. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 35, wobei das Verfahren als Voraussetzung für das Senden der Zahlungsanfrage ein erfolgreiches Erfassen und Validieren von ein oder mehreren vordefinierenden Sicherheitsmerkmalen (110) der Mehrmals von Sicherheitsmerkmalen (110) der Banknote (100) umfasst.

37. Verfahren zur Zahlungsabwicklung nach einem der Ansprüche 28 bis 36, wobei eine Mehrzahl von Banknoten (100) empfangen wird, wobei für jede der Banknoten (100) jeweils ein aktueller Nominalwert (109) ermittelt wird, wobei aus der Mehrzahl von empfangenen Banknoten (100) ein Satz von Banknoten (100) ausgewählt und einbehalten wird, deren aufsummierte aktuelle Nominalwerte (109) einen Betrag ergeben, der kleiner als ein zu zahlender Betrag ist, wobei ein verbleibender Differenzbetrag zwischen dem zu zahlenden Betrag und dem aufsummierten Betrag des Satzes von ausgewählten Banknoten (100) kleiner als ein aktueller Nominalwert (109) einer weiteren Banknote (100) der Mehrzahl von Banknoten (100) ist, welche nicht von dem Satz von ausgewählten Banknoten (100) umfasst ist, wobei die Zahlungsanfrage zur Zahlung des Differenzbetrags an die weitere Banknote (100) gesendet wird.

Es folgen 10 Seiten Zeichnungen

Anhängende Zeichnungen

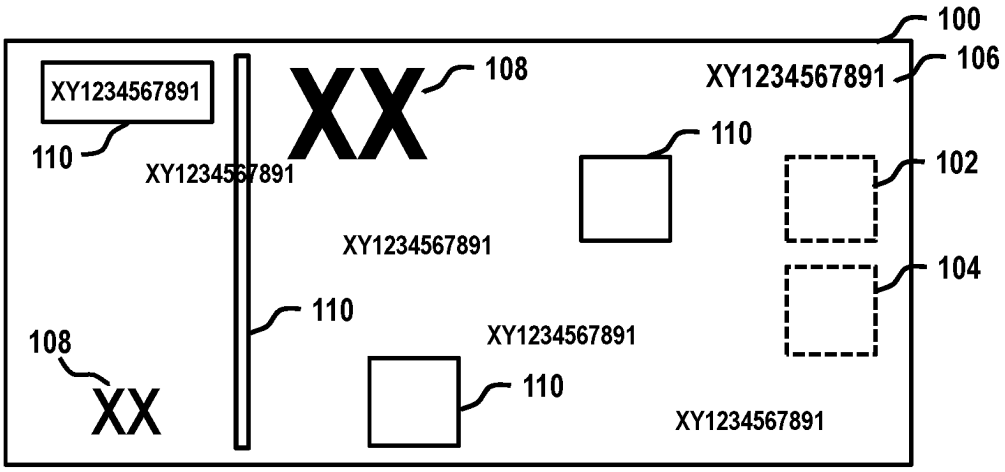


Fig. 1A

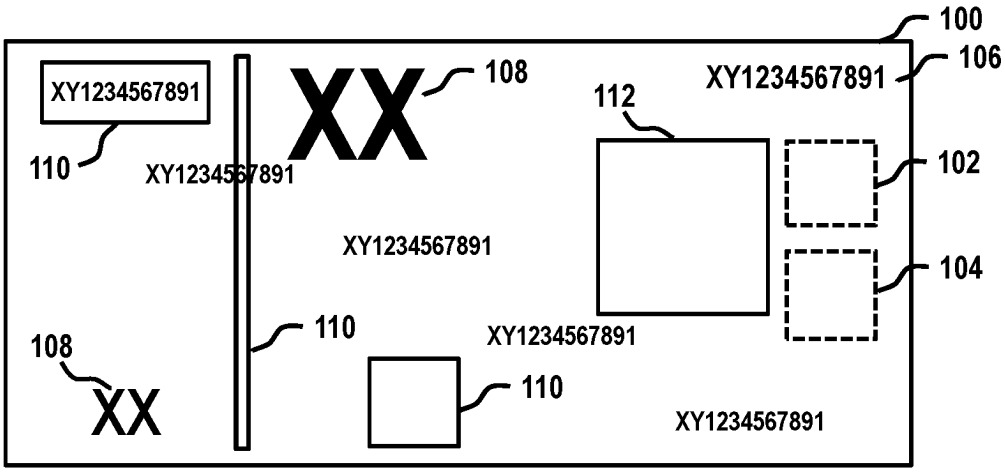


Fig. 1B

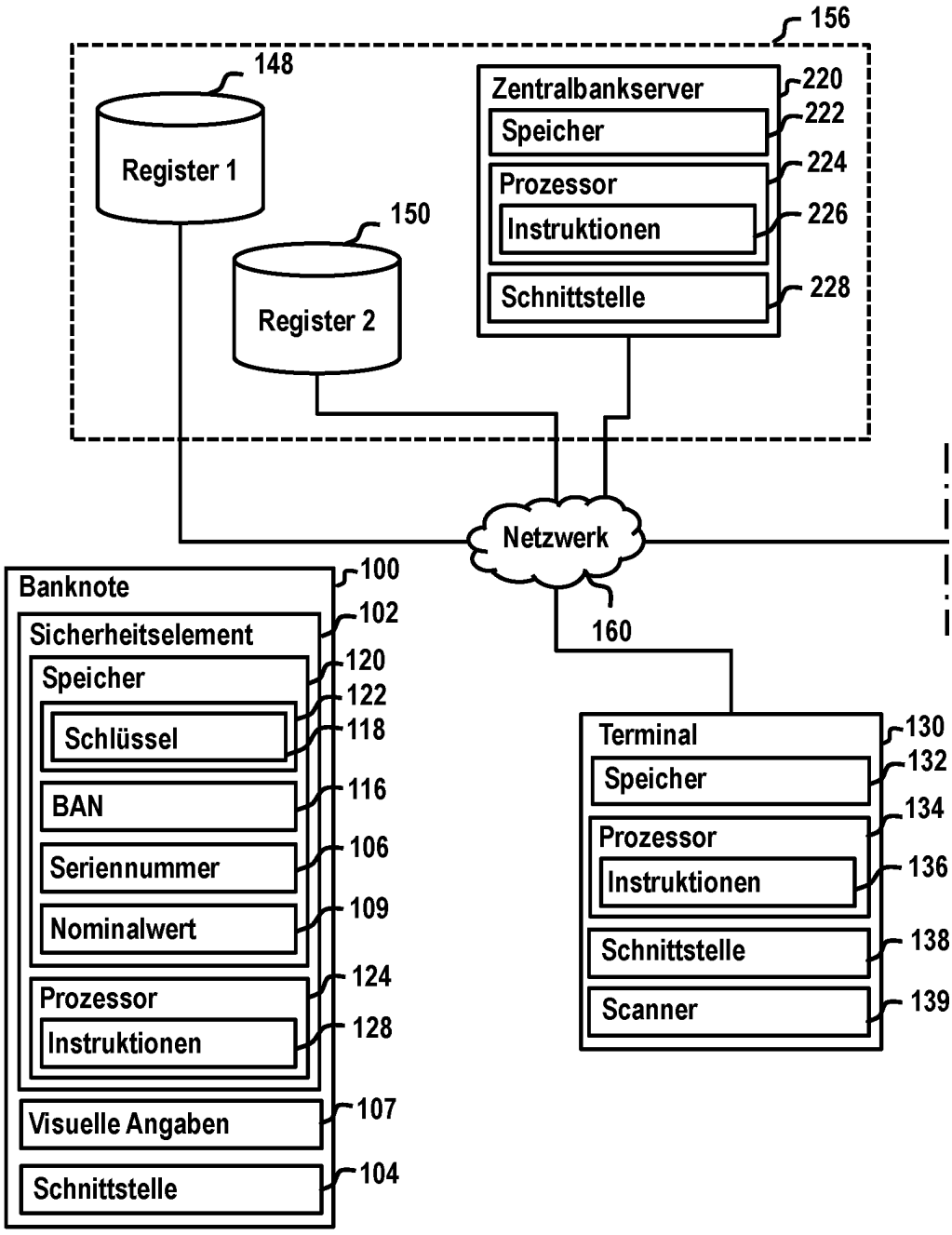

156
148
Register 1
150
Register 2
Zentralbankserver
220
Speicher
222
Prozessor
224
Instruktionen
226
Schnittstelle
228
Netzwerk
160
Banknote
100
Sicherheitselement
102
Speicher
120
Schlüssel
122
118
BAN
116
Seriennummer
106
Nominalwert
109
Prozessor
124
Instruktionen
128
Visuelle Angaben
107
Schnittstelle
104
Terminal
130
Speicher
132
Prozessor
134
Instruktionen
136
Schnittstelle
138
Scanner
139

Fig. 2A

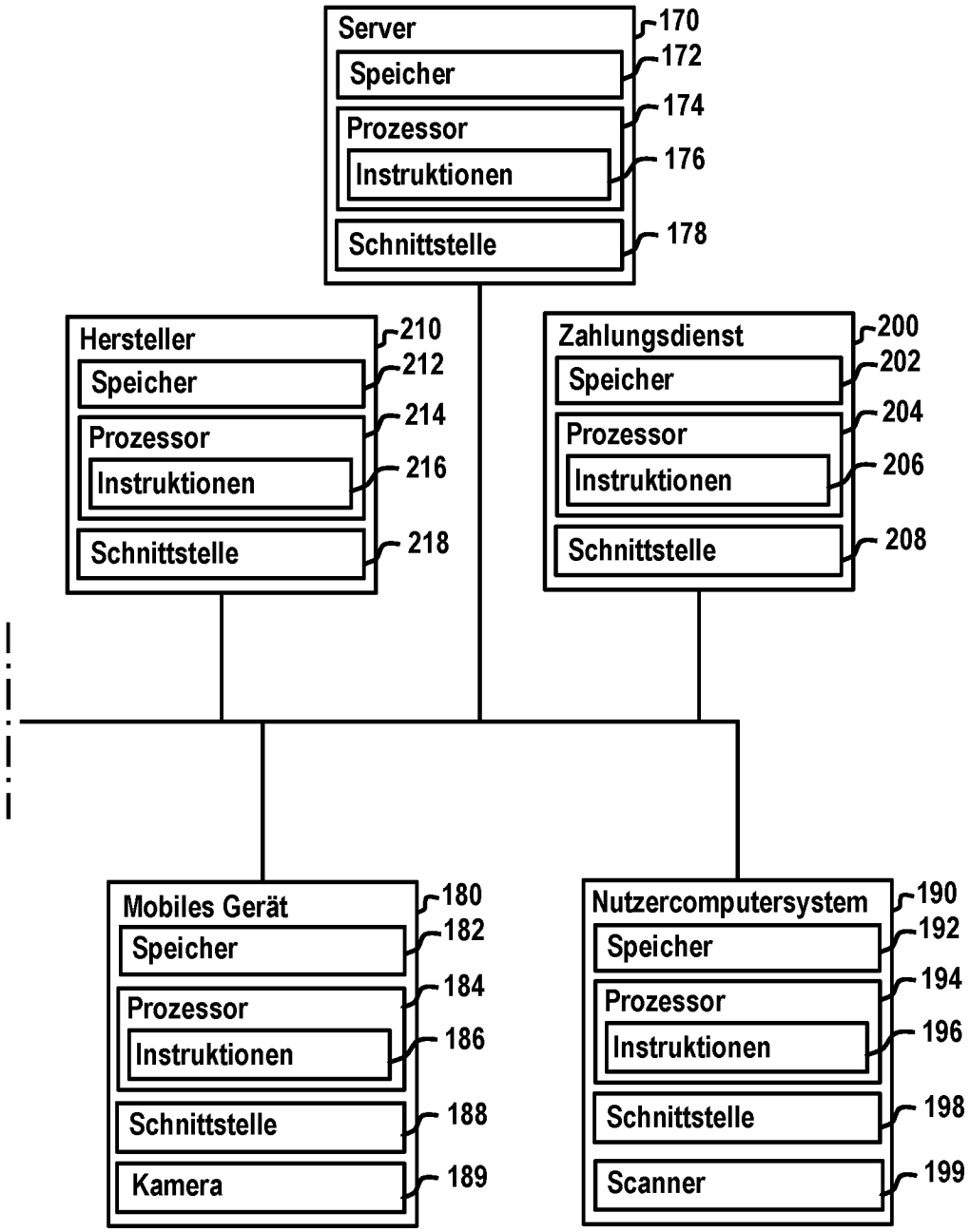

Server
170
Speicher
172
Prozessor
174
Instruktionen
176
Schnittstelle
178
Hersteller
210
Speicher
212
Prozessor
214
Instruktionen
216
Schnittstelle
218
Zahlungsdienst
200
Speicher
202
Prozessor
204
Instruktionen
206
Schnittstelle
208
Mobiles Gerät
180
Speicher
182
Prozessor
184
Instruktionen
186
Schnittstelle
188
Kamera
189
Nutzercomputersystem
190
Speicher
192
Prozessor
194
Instruktionen
196
Schnittstelle
198
Scanner
199

Fig. 2B

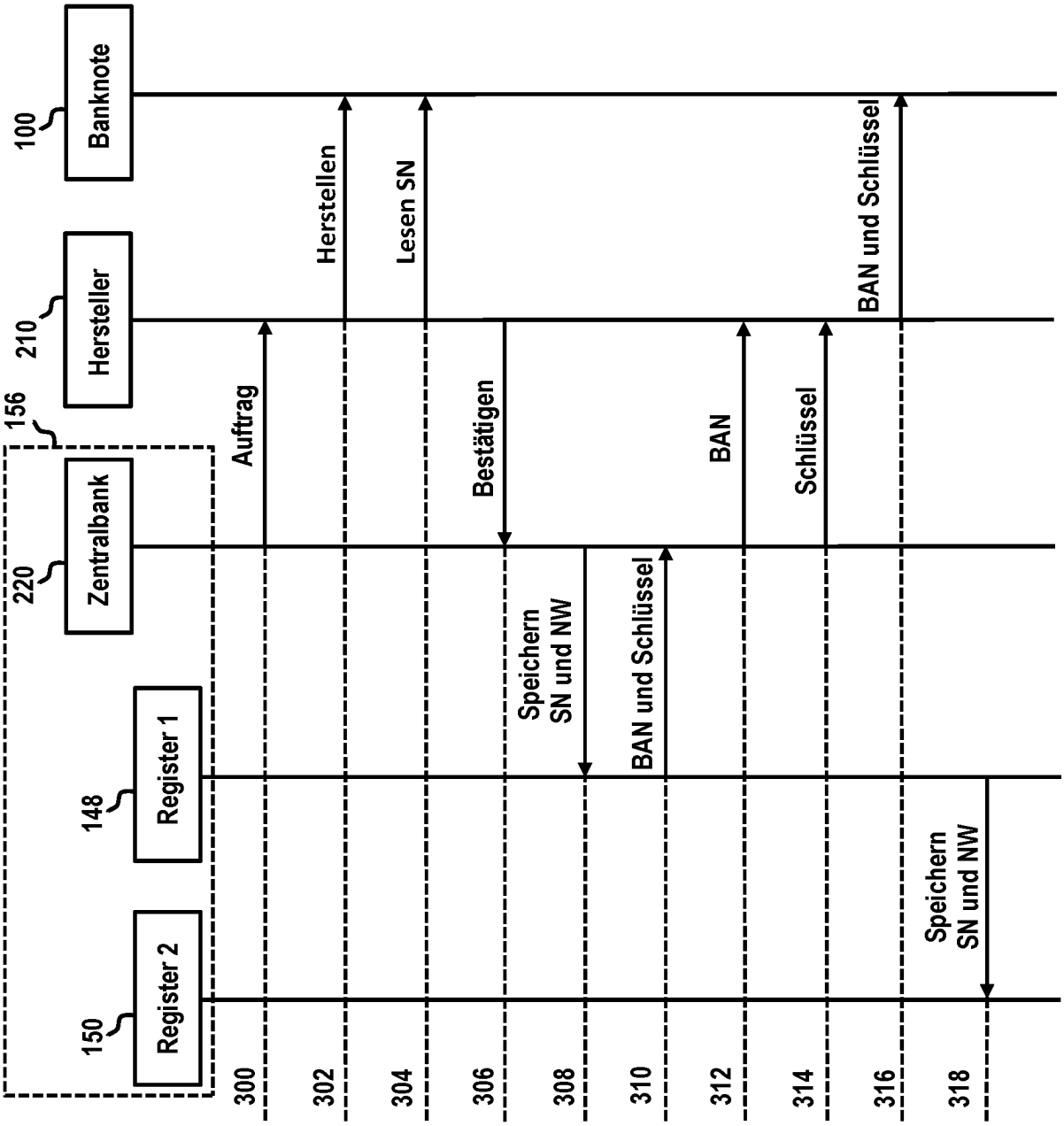

100
Banknote
210
Hersteller
156
220
Zentralbank
148
Register 1
150
Register 2
Auftrag
Herstellen
Lesen SN
Bestätigen
Speichern SN und NW
BAN und Schlüssel
BAN
Schlüssel
BAN und Schlüssel
Speichern SN und NW
300
302
304
306
308
310
312
314
316
318

Fig. 3

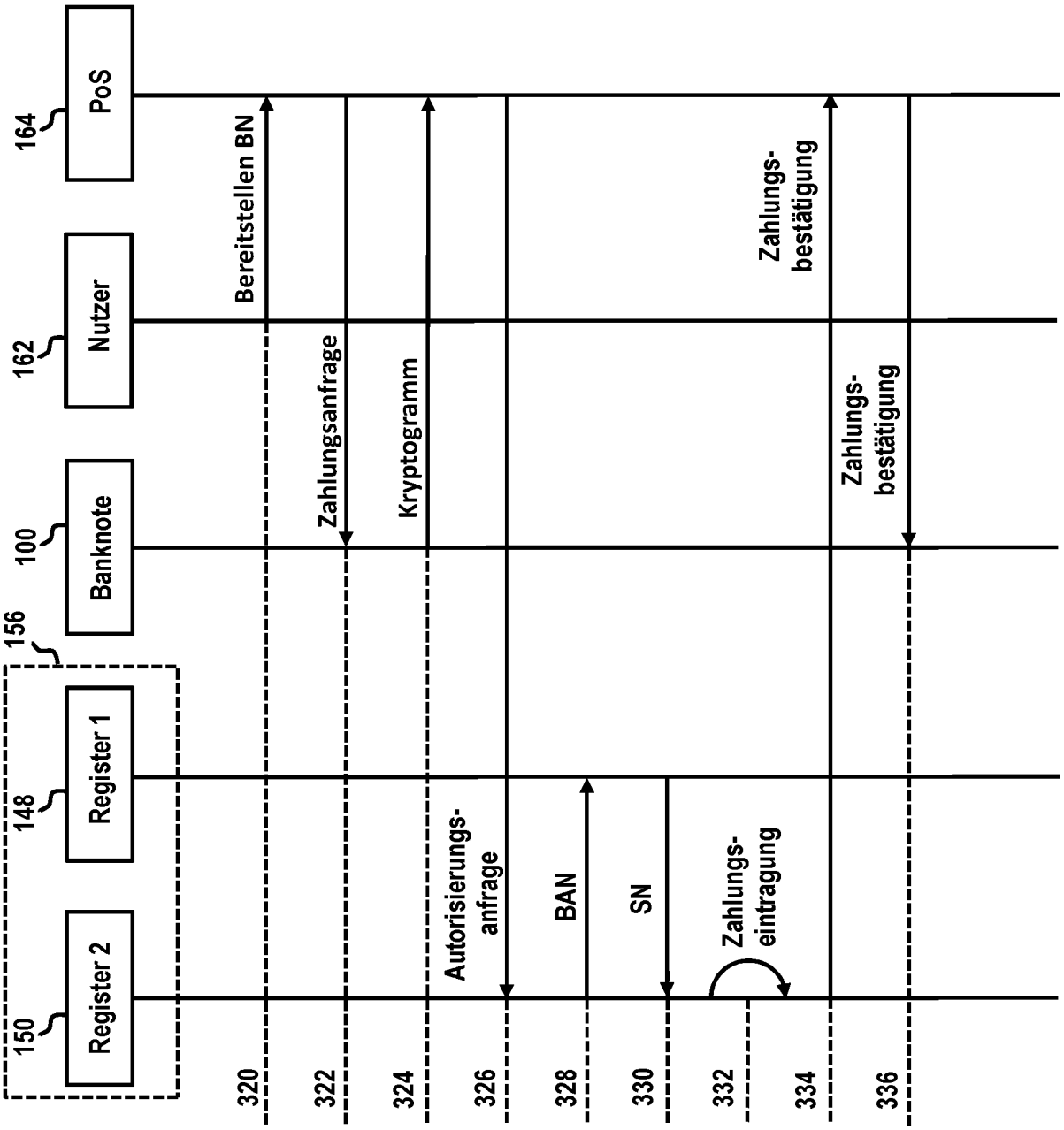

PoS
164
Nutzer
162
Banknote
100
156
Register 1
148
Register 2
150
Bereitstellen BN
Zahlungsanfrage
Kryptogramm
Autorisierungs-anfrage
BAN
SN
Zahlungs-eintragung
Zahlungs-bestätigung
Zahlungs-bestätigung
320
322
324
326
328
330
332
334
336

Fig. 4

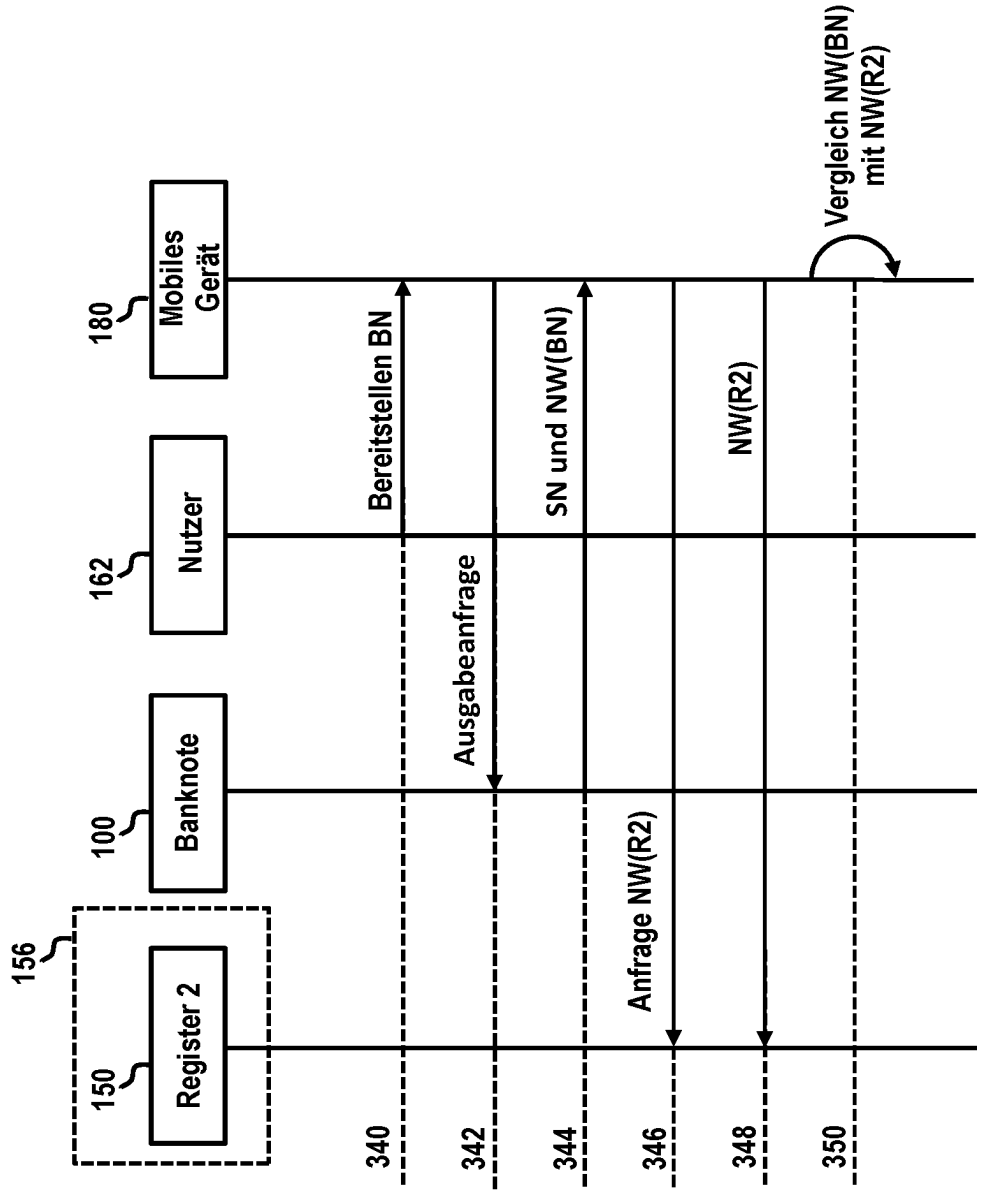

Vergleich NW(BN) mit NW(R2)
180
Mobiles Gerät
162
Nutzer
100
Banknote
156
150
Register 2
Bereitstellen BN
Ausgabeanfrage
SN und NW(BN)
Anfrage NW(R2)
NW(R2)
340
342
344
346
348
350

Fig. 5

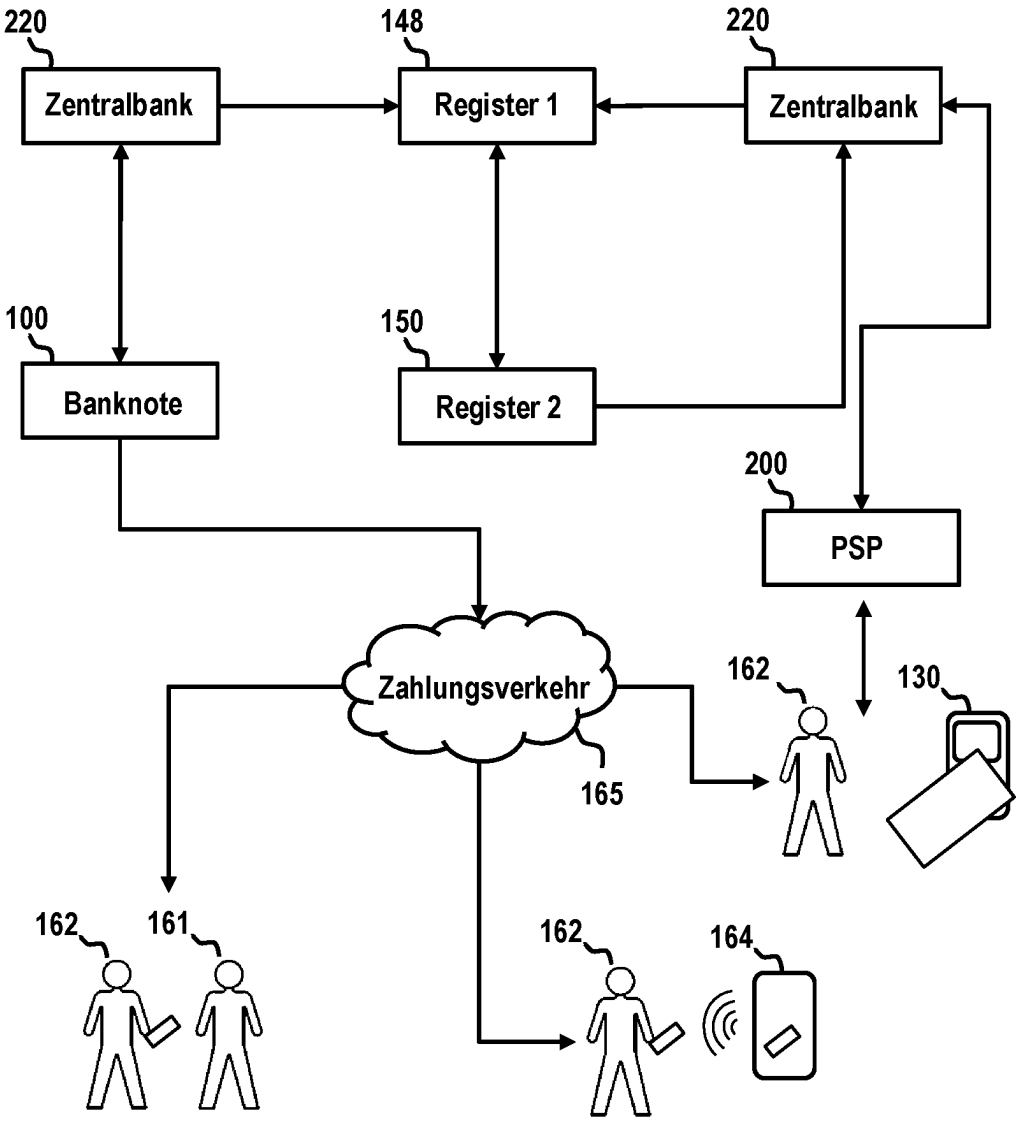

220
Zentralbank
148
Register 1
220
Zentralbank
100
Banknote
150
Register 2
200
PSP
Zahlungsverkehr
165
162
130
162
161
162
164

Fig. 6

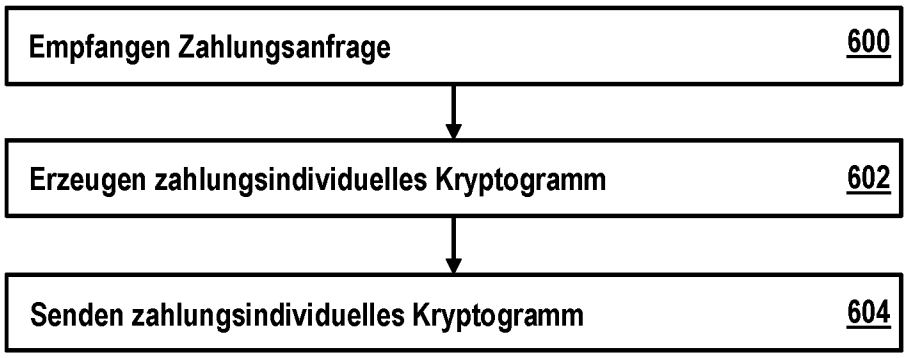

Empfangen Zahlungsanfrage
600
Erzeugen zahlungsindividuelles Kryptogramm
602
Senden zahlungsindividuelles Kryptogramm
604

Fig. 7

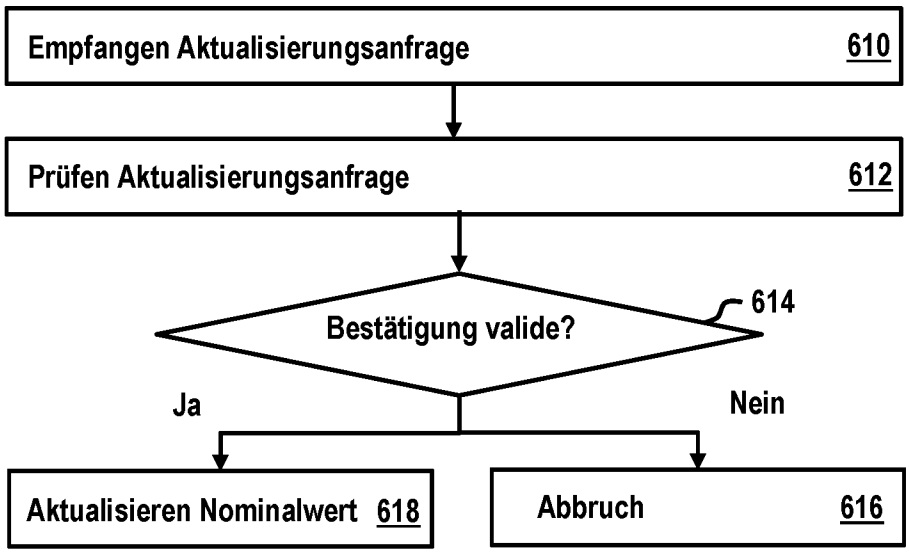

Empfangen Aktualisierungsanfrage
610
Prüfen Aktualisierungsanfrage
612
Bestätigung valide?
614
Ja
Nein
Aktualisieren Nominalwert
618
Abbruch
616

Fig. 8

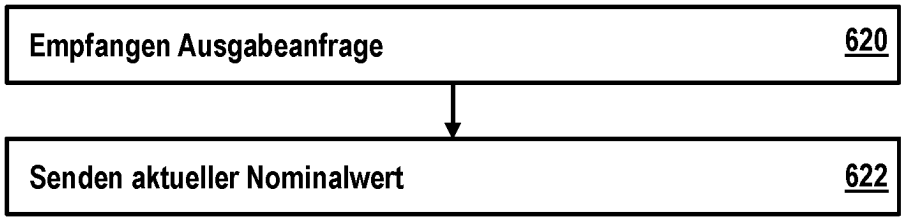

Empfangen Ausgabeanfrage
620
Senden aktueller Nominalwert
622

Fig. 9

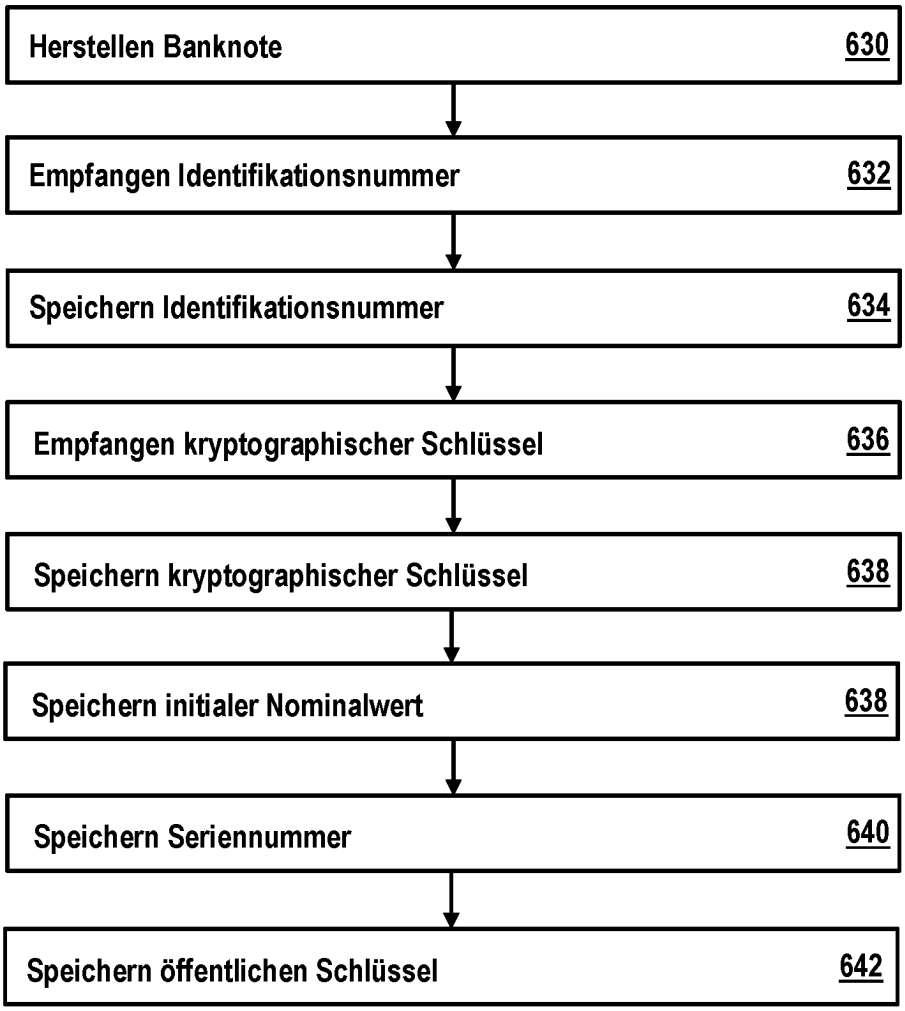

Herstellen Banknote
630
Empfangen Identifikationsnummer
632
Speichern Identifikationsnummer
634
Empfangen kryptographischer Schlüssel
636
Speichern kryptographischer Schlüssel
638
Speichern initialer Nominalwert
638
Speichern Seriennummer
640
Speichern öffentlichen Schlüssel
642

Fig. 10

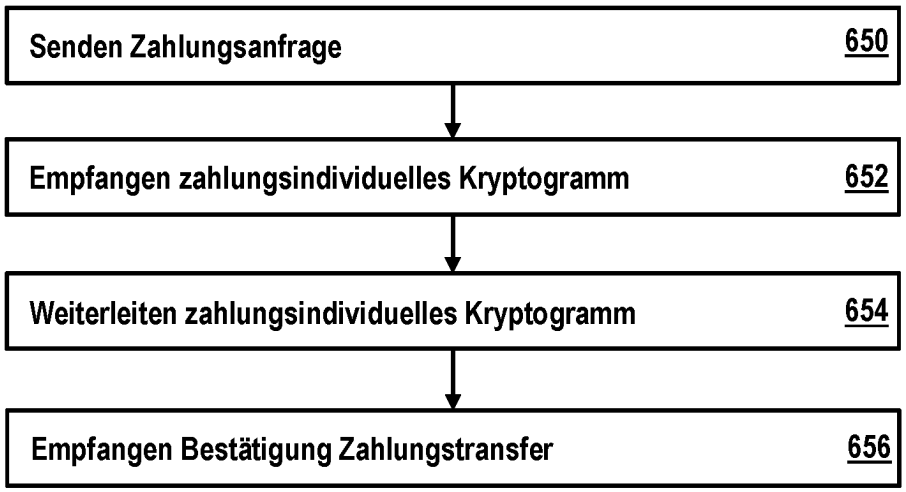


Fig. 11

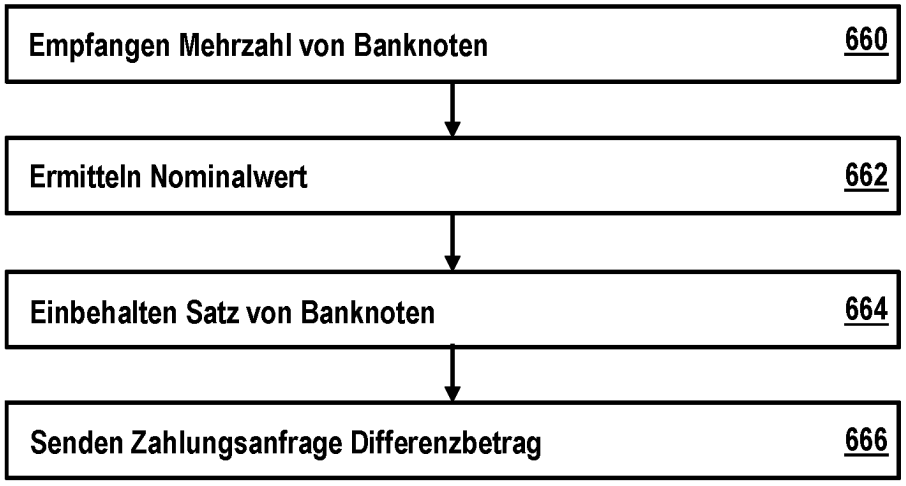


Fig. 12

