(19) Deutsches Patent- und Markenamt

(10) **DE 20 2020 001 476 U1** 2020.08.06

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2020 001 476.1**
(22) Anmeldetag: **09.04.2020**
(47) Eintragungstag: **29.06.2020**
(45) Bekanntmachungstag im Patentblatt: **06.08.2020**

(51) Int Cl.: ***G06K 19/04*** (2006.01)
G06Q 20/00 (2012.01)

(73) Name und Wohnsitz des Inhabers:
Potthoff, Oliver, Dipl.-Chem., 58579 Schalksmühle, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Vorrichtung zur Überführung von kryptographischen Werten, Token oder Coins in kryptographisches Bargeld ohne benötigter Energieversorgung des Bargeldes**

(57) Hauptanspruch: Physischer Hohlkörper in beliebiger Form, bevorzugt in Form eines Umschlages oder Münze aus Holz, Metall, Keramik, PVC, Papier, Pappe, Polyresin, Kunststoff oder ähnlicher geeigneter Materialien dadurch gekennzeichnet, dass der zur Einzahlungsadresse (Public Key) gehörende Seed einer Kryptowährung wie z.B. IOTA sich als Cold Wallet im Innerem des Hohlkörpers befindet und man nur an diesen gelangt, wenn man den Hohlkörper zerstört, bzw. aufbricht. Die Cold Wallet besteht aus den Zeichen des Seeds aufgebracht auf einem geeignetem Material wie z.B. Papier, Metall, Kunststoff oder ähnlichem. Diese zusätzlich versiegelte Cold Wallet, z.B. mit dem Kinebar Verfahren, wurde automatisiert bei der Fertigung des Hohlkörpers in diesen hinein gefertigt, verschlossen und ebenfalls mit einem geeignetem Verfahren versiegelt und nirgends abgespeichert und somit keiner Person bekannt. Die zugehörige Einzahlungsadresse, Public Key, ist außen auf dem Hohlkörper angebracht, mittels Adresscode oder z.B. als scanbarer 2D Code und dient zusätzlich zu den Siegeln der Überprüfung des hinterlegten Wertes auf der angegebenen Adresse, welche zu dem inne liegenden Seed gehört.

Beschreibung

[0001] Spätestens mit dem Erscheinen kryptografischer Werte wie dem Bitcoin im Jahre 2010 und vermehrt terroristischer Aktivitäten in der Welt, wird oftmals die Forderung nach der Abschaffung des Bargeldes, gerade in Regierungskreisen, immer lauter. Ein Argument der Gegner ist, dass dadurch es zu einer totalen Überwachung der Menschen kommen würde, da bei kryptographischen Werten der Token- oder Coinfluss in der Blockchain oder dem Tangle, im Falle von IOTA, nachvollzogen werden kann. Diese Tatsache birgt auch die Gefahr der Entstehung sogenannter verschmutzter Token oder Coins. Verschmutzte digitale Werte im Falle von z.B. IOTA können im Tangle identifiziert werden, als Werte die in der Vergangenheit bereits z.B. bei Straftaten eine Rolle spielten und somit als „verschmutzt“ bezeichnet werden und so u.U. den akzeptierten Wert der Token in der Gesellschaft reduzieren könnten. Sogenannte Mixer Services, die die Herkunft der Token oder Coins noch verschleiern können laufen allerdings Gefahr in der Zukunft verboten werden zu können.

[0002] Mit der vorliegenden Erfindung wird für beide Seiten, also den Befürwortern und den Gegnern der Abschaffung von Bargeld, eine Lösung gegeben durch eine Überführung kryptographischer Werte in nicht komplett verfolgbares kryptographisches Bargeld und dessen anschließende mögliche Rücküberführbarkeit in wieder rein kryptographische Token oder Coins. Gesetzliche Regelungen können z.B. anschließend festlegen bei welchen Vorgängen kryptographisches Bargeld verwendet werden darf und bei welchen zwingend die kryptographische Währung zu benutzen ist.

[0003] Die folgende Darstellung zur Herstellung kryptographischen Bargeldes erfolgt beispielhaft mit dem digitalen Bezahlsystem von IOTA, einem direkten azyklischem Graphen (DAG) und dem zugehörigem Tangle mit Public Key als Adresse für Einzahlungen und dem Seed zur Herrschaft über den Wert auf der Adresse. Die Vorrichtung gilt analog auch bei sämtlichen anderen dafür geeigneten kryptographischen Wertsystemen mit Blockchain und wird hier nur beispielhaft mit IOTA erklärt.

[0004] Bei der Herstellung von IOTA Bargeld durch eine dafür z.B. autorisierte Instanz wird zunächst automatisiert ein Seed erstellt im IOTA Tangle und ein sogenannter Public Key, der die öffentlich bekannte Einzahladresse darstellt.

[0005] Dieser Seed wird nun automatisiert versiegelt und in einen Umschlag gesteckt und anschließend auch der Umschlag verschlossen und versiegelt, so dass bis zu diesem Zeitpunkt niemanden der Seed bekannt ist und auch dieser nicht woanders abgespeichert wurde außer auf dem versiegelten Seed (Cold Wallet) in dem verschlossenen und versiegeltem Umschlag. Die von der Instanz verwendeten Siegel sind hierbei so angebracht, dass sie die Echtheit des Umschlages und auch seine Unversehrtheit garantieren können. Hierbei können u.a. die gewohnten Sicherheitsmerkmale verwendet werden, die auch traditionell bei gewöhnlichen Bargeldsystemen verwendet werden wie z.B. Reliefschrift, Wasserzeichen, Hologramm, Kinebar und/oder ähnliches geeignetes Verfahren aus dem aktuellem Stand der Technik.

[0006] Außen auf dem Umschlag wird nun der 2D Code und/oder nur die Zeichenfolge der Einzahlungsadresse bzw. Public Key aufgedruckt, sowie das von der ausgebenden Instanz des Kryptobargeldes eingezahlten Initial Betrages, z.B. 100 IOTA oder aber auch 0 IOTA im Falle einer Leergeldhülle für weitere Einzahlungen. So kann mit dieser Vorrichtung aus versiegelten Umschlag mit inne liegenden versiegelten und unbekannten Seed und außen angebrachten Public Key und aufgedruckten Betrag die Menge an hinterlegten Token auf der zum inne liegenden Seed gehörigen öffentlichen Adresse durch Scanen und Abfragen dieser das angegebene Guthaben auf dieser Adresse überprüft werden. Die Vorrichtung bietet so nun auch die Möglichkeit den außen auf dem Umschlag angegebenen Betrag zu erhöhen durch eine Einzahlung an den aufgebrachten Public Key bzw. der Einzahlungsadresse. So lange der Umschlag versiegelt bleibt, kann dieser von einer Person an eine weitere Person im Tausch gegen z.B. eine Ware oder Dienstleistung gehandelt werden wie traditionelles Bargeld auch. Der Empfänger des Kryptobargeldes, hier also des versiegelten Umschlages mit inne liegenden unbekannten Seed zu der außen aufgebrachten Einzahlungsadresse, versichert sich über die Echtheitsmerkmale und der Siegel, dass der Seed bisher keiner Person bekannt ist und auch wirklich sich in diesem Umschlag befindet. Weiter kann der Empfänger nun zusätzlich durch Abfrage der Adresse prüfen, ob auch wirklich der auf dem Umschlag angegebene Betrag sich auf der angegebenen Adresse befindet. Ist beides der Fall, die Siegel und Echtheitsmerkmale sind ungebrochen und als echt identifiziert und der Betrag befindet sich auch auf der Adresse die außen auf dem Umschlag angegeben ist, akzeptiert der Empfänger den Umschlag mit inne liegenden Seed als Wertsystem über den Betrag auf der Adresse ohne den Seed kennen zu müssen. Der Empfänger übergibt nun dem Überbringer des Umschlages die entsprechende Ware oder Dienstleistung, womit der Handel abgeschlossen wäre.

[0007] Dieser Handel wäre nun im Falle der Kryptowährung IOTA nicht im Tangle registriert oder analog bei anderen Krypto Zahlungssystemem wie z.B. Bitcoin nicht auf der Blockchain. Somit wurde die Kryptowährung in Krypto Bargeld überführt und zwar so lange, bis der Umschlag geöffnet wird und der

Seed genutzt wird, um die Kryptowährung von der aktuellen Adresse zu einer anderen, neuen Adresse im Tangel oder analog auf der Blockchain zu versenden, welches das Kryptobargeld wieder zurück in die ursprüngliche Kryptowährung verwandeln würde mit den Rückverfolgbarkeitseigenschaften die der Tangle oder die Blockchain üblicherweise bieten.

[0008] Diese Form der Überführung kryptographischer Zahlungssysteme in kryptographisches Bargeld wird somit verschmutzte kryptographische Token oder Coins aber noch nicht säubern, da die auf dem Umschlag aufgebrachte und somit bekannte Einzahlungsadresse den in der Vergangenheit liegenden Token- oder Coinverlauf bis zur Überführung in das Kryptobargeld noch auf dem Tangle bzw. der Blockchain sichtbar macht. Zur Lösung dieses Problems wird bei der Herstellung des kryptographischen Bargeldes durch die Instanz auf das zusätzliche Aufbringen des Public keys bzw. der Einzahlungsadresse verzichtet und nur der Betrag aufgedruckt, über den man verfügen kann, wenn der im Umschlag inne liegende versiegelte Seed benutzt wird. Die Echtheit des Umschlages und somit das Vertrauen darauf, dass auch der aufgedruckte Betrag auf einer Adresse liegen, über die man durch den inne liegenden Seed verfügen kann, ergibt sich durch die von der ausgebenden Instanz verwendeten und geeigneten Sicherheitsmerkmale des Umschlages, wie es auch bei traditionellem Bargeld erreicht wird.

[0009] Der in Schutzanspruch 1 angegebenen Erfindung liegt das Problem zugrunde, eine Vorrichtung zu entwickeln, welche ein öffentliches und verfolgbares kryptographisches Zahlsystem in ein nicht verfolgbares Zahlsystem überführt und somit eine typische Eigenschaft des Bargeldes, den nicht ohne weiteres verfolgbaren Wertefluss, zu übernehmen.

[0010] Der in Schutzanspruch 2 angegebenen Erfindung liegt das Problem zugrunde, eine Vorrichtung zu entwickeln, welche zusätzlich zu den in Schutzanspruch 1 angegebenen Erfindung, das Problem löst auch den vorherigen Werteverlauf des zu überführenden Kryptowertes, bis zum Zeitpunkt der Überführung ein nicht weiter verfolgbares Zahlsystem, unkenntlich macht und somit sogenannte „verschmutzte Coins oder Token“ säubert und somit die Eigenschaften des Bargeldes, den nicht verfolgbaren öffentlichen Wertefluss vor- und nach der Überführung in das Krypto Bargeld zu gewährleisten. Durch die Vorrichtung entsteht kryptographisch abgedecktes Bargeld. Staaten haben somit auch die Möglichkeit eigenes kryptographisches Bargeld herauszugeben in gewünschter Stückelung und bei z.B. IOTA oder Ethereum zusätzlich die Möglichkeit diese in die entsprechende Landeswährung über colored Token einzufärben.

Schutzansprüche

1. Physischer Hohlkörper in beliebiger Form, bevorzugt in Form eines Umschlages oder Münze aus Holz, Metall, Keramik, PVC, Papier, Pappe, Polyresin, Kuststoff oder ähnlicher geeigneter Materialien **dadurch gekennzeichnet**, dass der zur Einzahlungsadresse (Public Key) gehörende Seed einer Kryptowährung wie z.B. IOTA sich als Cold Wallet im Innerem des Hohlkörpers befindet und man nur an diesen gelangt, wenn man den Hohlkörper zerstört, bzw. aufbricht. Die Cold Wallet besteht aus den Zeichen des Seeds aufgebracht auf einem geeignetem Material wie z.B. Papier, Metall, Kunststoff oder ähnlichem. Diese zusätzlich versiegelte Cold Wallet, z.B. mit dem Kinebar Verfahren, wurde automatisiert bei der Fertigung des Hohlkörpers in diesen hinein gefertigt, verschlossen und ebenfalls mit einem geeignetem Verfahren versiegelt und nirgends abgespeichert und somit keiner Person bekannt. Die zugehörige Einzahlungsadresse, Public Key, ist außen auf dem Hohlkörper angebracht, mittels Adresscode oder z.B. als scanbarer 2D Code und dient zusätzlich zu den Siegeln der Überprüfung des hinterlegten Wertes auf der angegebenen Adresse, welche zu dem inne liegenden Seed gehört.

2. Physischer Hohlkörper in beliebiger Form, bevorzugt in Form eines Umschlages oder Münze aus Holz, Metall, Keramik, PVC, Papier, Pappe, Polyresin, Kuststoff oder ähnlicher geeigneter Materialien **dadurch gekennzeichnet**, dass der zur Einzahlungsadresse (Public Key) gehörende Seed einer Kryptowährung wie z.B. IOTA sich als Cold Wallet im Innerem des Hohlkörpers befindet und man nur an diesen gelangt, wenn man den Hohlkörper zerstört, bzw. aufbricht. Die Cold Wallet besteht aus den Zeichen des Seeds aufgebracht auf einem geeignetem Material wie z.B. Papier, Metall, Kunststoff oder ähnlichem. Diese zusätzlich versiegelte Cold Wallet, z.B. mit dem Kinebar Verfahren, wurde automatisiert bei der Fertigung des Hohlkörpers in diesen hinein gefertigt, verschlossen und eben falls mit einem geeignetem Verfahren versiegelt und nirgends abgespeichert und somit keiner Person bekannt. Die zugehörige automatisch erstellte Einzahlungsadresse, Public Key, ist ebenfalls niemandem bekannt und wird anders als im Anspruch 1 nicht außen auf den Umschlag gedruckt.
Bei der Seed Erstellung wird automatisiert eine Einzahlungsadresse erstellt und auch auf diese der Betrag eingezahlt, den die autorisierte Institution anschließend auf den Umschlag außen aufdruckt. Diesem aufgedruckten Betrag wird nun durch die Sicherheitsmerkmale vertraut und der Betrag ist durch den im Umschlag hinterlegten Seed kryptographisch abgesichert bzw. abgedeckt. Durch die Vorrichtung entsteht kryptographisch abgedecktes Bargeld.
Staaten haben somit auch die Möglichkeit eigenes kryptographisches Bargeld herauszugeben in ge-

wünschter Stückelung und bei IOTA zusätzlich die Möglichkeit diese in die entsprechende Landeswährung über colored Token einzufärben.

Es folgen keine Zeichnungen