

Computer basiertes System und Verfahren zur Vermittlung von Partnerkontakten

Die Erfindung bezieht sich auf ein Computer basiertes System zur Nutzung von bereitgestellten, personenbezogenen Datensätzen zur manipulationsgeschützten und Datenschutzkonformen Partnervermittlung zwischen einander bekannten und unbekanntem Nutzern durch Verwendung einer verteilten dezentralen Datenbank.

Systeme zur Partnervermittlung (sog. Dating-Portale) beruhen auf dem Prinzip, Individuen basierend auf verschiedenen Gemeinsamkeiten miteinander zu verbinden. Im Allgemeinen ermöglichen es die Systeme einzelnen Individuen, ein Benutzerprofil auf einer Website zu erstellen. Das Benutzerprofil kann soziale Vernetzungsinformationen enthalten, die durch den Benutzer spezifiziert werden können. Diese betreffen zum Beispiel biografische Informationen wie Name, Alter, Geschlecht usw., bildungsbezogene Informationen wie Schulen, Berufsabschlüsse usw., persönliche Informationen wie Interessen, Hobbys, Beziehungsstatus usw. Soziale Vernetzungsinformationen, die in Benutzerprofilen enthalten sind, können durch ein soziales Vernetzungssystem verwendet werden, um Übereinstimmungen zwischen Individuen zu erzeugen und diese in Verbindung zu bringen.

Das jeweilige Benutzerprofil kann auch digitale Mediendateien wie Fotografien, Filme oder Tonaufnahmen enthalten, die durch den Benutzer ausgewählt und in das Benutzerprofil hochgeladen werden. Digitale Mediendateien können durch eine Kamera, eine Videokamera, ein Smartphone oder eine andere Vorrichtung aufgenommen werden, die zum Erstellen einer digitalen Mediendatei geeignet ist. Diese Vorrichtungen können eine Internetanschlussmöglichkeit aufweisen und es ermöglichen, die digitalen Mediendateien über die Website des sozialen Vernetzungssystems direkt in das Benutzerprofil hochzuladen.

Online Dating-Portale sehen sich vielen Problemen gegenübergestellt. Wenn ihre Nutzer gefälschte Daten ungeprüft über ihre Plattform ins Internet stellen, wie z.B. gefälschte oder gestohlene Fotos, ist die Bewertung der rechtlichen Lage bspw. die Haftung bei einem entstandenen Schaden sehr ungewiss. Prüft dagegen die

Dating-Agentur die Daten und Bilder ihrer Nutzer ausreichend, müssen diese Daten zum einem in Übereinstimmung mit den Regelungen der Datenschutzgrundverordnung, also DSGVO konform, vertraulich behandelt werden. Zum anderen müssen die Daten aber zur Vermittlung eines geeigneten Partners anderen Interessenten vorgestellt werden.

Auf der Seite der Nutzer des Dating-Portals entstehen auch eines oder mehrere der folgenden Probleme: Die eigenen Daten müssen einer zentralen Instanz, der Dating-Agentur, anvertraut werden, welche diese zentral speichert. Bevorzugt man Plattformen, welche die Bilder der Kunden nicht überprüfen, läuft man selbst Gefahr auf ein gefälschtes oder gestohlenen Bild seines Gegenübers herein zu fallen. Stellt man aber selbst sein Bild ehrlich online in die Kartei des Anbieters, läuft man Gefahr, dass andere sehen, dass man selbst auf der Partnersuche ist. Je strenger die Prüfung des Dating-Portals ist, desto höhere Kosten entstehen, die auf die Nutzer des Dating-Portals umgelegt werden müssen. Hinzu kommt bei der zentralen Speicherung der Daten das Risiko, dass von Unbefugte unerlaubt in die Datenbank eindringen und Daten und folglich auch Bilder stehlen.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, die vorgenannten Probleme zu beseitigen und eine für Betreiber und Nutzer der Dating-Portale sichere und zuverlässige Gestaltung zu schaffen. Gemäß der Erfindung wird diese Aufgabe mit den Merkmalen des Patentanspruchs 1 gelöst.

Mit der Erfindung ein Computer basiertes System zur Vermittlung eines Partnerkontaktes geschaffen, welches ein Höchstmaß an Datensicherheit für den Betreiber und die Nutzer ermöglicht und gleichzeitig ein sehr hohes Maß an erfolgreichen Vermittlungen erzielt.

Erfindungsgemäß bekommt eine Person A die Person B erst zu sehen und Person B erst die Person A zu sehen, nachdem man bereits weiß, dass sich beide zu einer sehr hohen Wahrscheinlichkeit gegenseitig optisch und charakterlich attraktiv finden werden. Die Bilder und Daten der Personen A und B sind dabei zu keiner

Zeit irgendwo zentral gespeichert oder gar einer dritten Instanz zugänglich, außer den Eigentümern dieser Daten, nämlich den Personen A und B selbst.

Die vorliegende Erfindung ist dadurch in der Lage, die genannten Probleme zu lösen und liefert dabei ein System, wie Person A erst für eine bewusste Begegnung mit Person B sichtbar wird, nachdem bekannt ist, dass Person A mit einer hohen Wahrscheinlichkeit Person B optisch attraktiv finden wird und Person B im Gegenzug auch Person A optisch attraktiv finden wird. Zusätzlich wird dabei auch darauf geachtet, dass beide Personen auf vielen Ebenen für eine erfolgreiche zukünftige Partnerschaft passende Vorstellungen und Charaktereigenschaften besitzen. So würde z.B. Person A mit ausgeprägtem Kinderwunsch keinen Partner zugeordnet bekommen, der keine Kinder möchte. Sämtliche Daten der beteiligten Personen werden dabei kryptographisch verschlüsselt. Die Kryptographie ist eine Methode, Daten in einer bestimmten Form zu sichern und zu übertragen, so dass nur diejenigen Personen, für die sie bestimmt sind, die Daten lesen und verarbeiten können. Dadurch ist ein Höchstmaß an Sicherheit geschaffen, welches herkömmliche Dating-Portale nicht aufweisen. In jedem Fall werden die Personen erst für andere sichtbar, nachdem eine sehr hohe Übereinstimmung in den jeweils festgelegten Kriterien vorliegt. Dadurch ist für die übrigen Nutzer des Dating-Portals nicht sichtbar, wer auf der Suche nach einem Partner ist.

Neben der Verschlüsselung werden die Daten dezentral abgespeichert und können nur mit einem privaten Schlüssel angesehen werden, der ausschließlich in den Händen der jeweils berechtigten Person liegt. Die Speicherung der Daten erfolgt dabei dezentral durch Nutzung des IOTA Tangle Netzwerkes. IOTA steht für ein Protokoll, das sich der Kommunikation zwischen Maschinen verschrieben hat. IOTA basiert nicht auf einer „herkömmlichen“ Ketten- also Blockchain-Technik. In einer Blockchain wird einer wachsenden Chain (Kette) von Blöcken periodisch ein neuer Block hinzugefügt. Jeder Block ist mit dem vorhergehenden Block durch eine Art kryptographische Verbindung verbunden (konkret durch einen Hash).

IOTA basiert dagegen auf einer sog. Distributed Ledger Technologie (DLT) namens Tangle („Gewirr“). Im Vergleich zu einer Blockchain ist der Tangle ein „chaotisches“ Netz mit sehr vielen Verknüpfungen. Sämtliche Transaktionen können parallel laufen. Eine weitere Besonderheit von IOTA ist der im Vergleich zu anderen Protokollen sehr geringe Stromverbrauch. Der Tangle ist dabei die Datenstruktur, die durch die Verbindungen zwischen Transaktionen im verteilten Ledger auf allen Nodes entsteht. Technisch ausgedrückt ist der Tangle ein directed acyclic graph - DAG (dt. gerichteter azyklischer Graph). Nodes sind Netzwerkknoten, welche Verbindungen zwischen Netzwerkelementen herstellen.

5
10

Das erfindungsgemäße System kann auf Wunsch kostenlos für die Nutzer sein. Dies kann durch das Schalten von Werbung in Abhängigkeit vom Erreichen verschiedener Zwischenziele oder der Durchführung verschiedener Schritte der Nutzer erreicht werden.

15

Eine Erklärung der Funktionsweise des erfindungsgemäßen Systems bzw. des Verfahrens stellt sich wie folgt dar.

1. Schritt Identitäts-Datenerhebung: Die persönlichen Daten der Nutzer des Portals wie Foto, Adresse, Alter etc. werden kryptographisch abgespeichert zur DID.

20

2. Schritt Datenerhebung Optik: Die gesuchte bevorzugte optische Attraktivität des potentiellen Partners wird auf Basis einer psychologischen Testtheorie im Labor bei den Nutzern ermittelt. Das ermittelte Bild wird jeweils als 100% Treffer oder 100% Match gesetzt. Im Anschluss werden die ermittelten Gesichtspunkte des Matchingpartners um das 100% Match variiert, so dass auch Gesichtspunktvariationen einbezogen werden, die nicht zu 100% dem gesuchten Traumgesicht entsprechen. So entstehen viele verschiedene sog. Hashwerte. Hashwerte sind dabei Prüfsummen, die für die Verschlüsselung von Nachrichten mit variabler Länge verwendet werden. So wird jeder Nachricht ein ganz bestimmter Hashwert zugeordnet. Ein Hashwert vereint in sich eine Vielzahl von Informationen, die über

25
30

eine Hashfunktion zugeordnet werden, wobei die Hashfunktion eine beliebig lange Zeichenabfolge übertragen kann. Hashwerte sind Fingerabdrücke eines sehr langen Datensatzes. Für jedes mögliche Gesicht innerhalb der Abweichung wird ein Hashwert gebildet. So könnte z.B. eine Einbeziehung von 98 bis 100% Gesichtspunktübereinstimmung 150 Gesichtsvariationen hervorbringen, entstanden aus den möglichen neuen Gesichtspunktvariationen um das 100% Match herum. Diese 150 Variationen bringen insgesamt 150 Hashes bzw. Hashwerte, welche zu einem Wurzelhash, also zu einem Hashwert aller Hashwerte aller Transaktionen zusammengefasst bzw. gehasht werden, dem sog. „Optik-Hash“.

10

3. Schritt Matchingerhebung: Per Smart Contracts / Oracles auf einer privaten Chain des Anbieters innerhalb des Tangle Netzwerks, wird nun untersucht, wessen Foto-Hashwert innerhalb der DID mit dem Optik-Hash eines potentiellen Partners übereinstimmt. Wenn der Hashwert, der die Gesichtspunkte von Person A kryptographisch verschlüsselt abspeichert innerhalb der 150 Hashes aus dem Optik-Hash von Person B vorkommt, dann folgt daraus, dass Person A mit seinen Gesichtspunktmerkmalen innerhalb der 98% Toleranzgrenze liegt, der von Person B als optisch am meisten bevorzugt empfunden wird. Mit anderen Worten: Das Aussehen von Person A entspricht zu mindestens 98% demjenigen, wie es von Person B als am attraktivsten empfunden angegeben wurde. Wenn dies umgekehrt ebenso der Fall ist, also der Hashwert zum Gesicht der Person B aus dessen DID ebenfalls innerhalb der Hashwertvariationen um die für Person A innerhalb der 98% Toleranzgrenze der als am attraktivsten ermittelten Gesichter in Form des entsprechenden Hashwertes liegt, ergibt sich ein Match, also zwei in Bezug auf das Aussehen nahezu perfekt zueinander passende Partner.

25

4. Schritt Kontaktvermittlung: Nun müssen Person A und Person B noch bekannt gemacht werden. Dies kann auf einem Smartphone geschehen, bspw. per installierter App, welche das dezentrale Tangle Netzwerk nutzt, wie z.B. Society2. Nutzer von Society2 sind in die Lage versetzt, eine digitale Identität, sprich ihr Social Media Profil, verschlüsselt auf dem IOTA Tangle Netzwerk zu verwalten. Society2 nutzt dies bereits zur dezentralen und anonymen Kommunikation. An die

30

Personen A und B können nun automatisiert jeweils eine Mitteilung gesendet werden und ein privater Chatraum geöffnet werden. Dies kann bspw. über einen Smart Contract erfolgen. Smart Contracts sind Computerprotokolle, die Verträge abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrags technisch unterstützen können. Eine schriftliche Fixierung des Vertrages (auf 5 Papier oder in einer Datei) wird damit in der Regel überflüssig. Smart Contracts haben üblicherweise auch eine Benutzerschnittstelle und bilden die Logik vertraglicher Regelungen technisch ab. Der Zutritt zu dem so eröffneten privaten Chat Raum ist dabei jeweils nur mit den beiden DID von Person A und Person B 10 möglich. Da ein Smart Contract Gebühren nach sich zieht, kann bspw. über Werbeeinnahmen auf der Anbieter-Plattform die entsprechende monetäre Kompensation erfolgen, so dass die Vermittlung für Person A und Person B komplett ohne Gebühren erfolgt.

15 Ergänzend kann in einer weiteren Stufe vor der Feststellung eines Matches von Person A und Person B bspw. noch die Frage erhoben werden, ob ein Kinderwunsch vorliegt. Über Smart Contracts könnten nun verschiedene Matchvariationen hinterlegt werden, bspw. nach dem Prinzip „Wenn Person A und Person B im Kinderwunsch nicht übereinstimmen, dann muss die Übereinstimmung in der opti- 20 schen Attraktivität bei 99,5% liegen.“

Auch können Person A und Person B über ein Globales Positionsbestimmungssystem (Global Positioning System GPS), offiziell NAVSTAR GPS genannt, bei dem es sich um ein globales Navigationssatellitensystem zur Positionsbestimmung 25 handelt, regelmäßig ihre Bewegungsdaten in den Tangle speisen, welche als Rückkopplungsfeedback zu dem erfolgten Match dienen. Auf diese Weise kann ermittelt werden, ob es z.B. mit höherer Übereinstimmung in der Attraktivität zu mehr gemeinsamen Begegnungen kommt und bei welcher Attraktivitätsübereinstimmung die Kinderfrage mehr oder weniger Einfluss auf die gemeinsamen 30 Begegnungen hat. Ein Smart Contract könnte bspw. folgendermaßen lauten: Wenn die Begegnungen aller zusammengeführter Nutzer im Schnitt weniger als X Stunden im Zeitraum Y betragen haben und ihre Übereinstimmung in der Attrakti-

5 vität im Mittel bei 99,5% lag, dann gilt die Zusammenführung der Nutzer als gescheitert und es werden zukünftig nur noch die gemeinsamen optischen Hashwerte der Personen A und B zusammengeführt (gematcht), wenn sie bei min. 99,6% Übereinstimmung liegen. So wäre bereits ein sehr einfacher selbstlernender Algorithmus auf dem IOTA Tangle in Form eines Oracles bzw. Smart Contracts auf einer Sidechain zu realisieren. Oracles sind dabei Agenten, die externe Daten auf die Blockchain bringen. Operationen, die auf der Blockchain ausgeführt werden, beispielsweise Smart Contracts, werden durch das dezentrale Netzwerk an Teilnehmern geprüft. Ein Sidechain ist eine Blockchain, der von einer übergeordneten
10 Blockchain abgespalten wurde und seither in gewissen Grenzen eigenständig arbeiten kann. Sie ist jedoch weiterhin mit ihrer ursprünglichen Blockchain verbunden, so dass z.B. ermittelte Ergebnisse (Assets) zwischen beiden Blockchain ausgetauscht werden können. Es wird so lange versucht, zulässige Lösungsmöglichkeiten zu ermitteln (sog. Try and Error), bis die gewünschte Lösung gefunden wurde. Durch solche Try and Error Algorithmen kann sich mit der Zeit das System
15 selbstlernend in Bezug auf ein als erfolgreich zu definierendes Match verbessern.

In einer weiteren Variante des Systems wird zunächst ein Optik-Hash von Person A aus dessen eigenen Optikdaten erstellt. Im nächsten Schritt werden die erhobenen Psycho-Physiologischen Matchingdaten von Person A zu einem Charakter-Hash transformiert. Anschließend wird der Charakter-Hash zusammen mit einem spezifischen Love2Tangle Hash und dem Optik-Hash zum finalen Wurzelhash, dem Love-Hash, überführt. Der Love Hash ist der finale Wurzelhash über alle zum Matchen notwendig erhobenen und verschlüsselten Daten von Person A. Der Love-Hash wird dann auf dem IOTA Tangle-Netzwerk abgespeichert.
20
25

Der Love-Hash ist zugleich der Zugangsschlüssel für Person A zum eigenen Chatraum, um diesen für die Öffentlichkeit zu erstellen. Dies ist durch den spezifischen Love2Tangle Hash gewährleistet, der eine Art „Wasserzeichen“ bildet. Er ist unter anderem von der DID gebildet sowie weiteren internen Größen, die eine eindeutige Identifizierung und damit auch eine Prüfung der Berechtigung zum Zutritt in einen Chatraum o.dgl. ermöglichen. Nun wird ein Chatraum Schloss erstellt, das
30

sich mit allen Love-Hashes von anderen Personen als Person A öffnen lassen wird, solange deren persönlicher Love-Hash innerhalb eines Bereichs von X% Abweichung von den matchenden Optik- und Charakterwertanforderungen zur Person A liegt. Hierzu werden alle möglichen zu X% maximal abweichenden Datenvarianten im Optik- und Charakterbereich jeweils in einen Hash-Wert überführt. 5 Alle so erhaltenen Hash-Werte aus den Kombinationen der Matchingdaten, die innerhalb der X% Abweichungstoleranz liegen, werden abschließend ebenfalls noch mit einem spezifischen Love2Tangle Hash zusammen zum finalen Wurzelhash überführt, dem Chatraumschloss-Hash von Person A. Dieser Wurzelhash 10 wird ebenfalls auf dem IOTA Tangle-Netzwerk abgespeichert. Nun kann, nachdem Person A den Chatraum mit ihrem persönlichen Zugangsschlüssel, dem Love-Hash von Person A, eröffnet hat jede weitere Person X probieren, ob sie mit ihrem persönlichen Love-Hash den Chatraum von Person A betreten kann. Dies ist nur möglich, wenn der Love-Hash von der Person X aus einer Datenkombination hervorgegangen ist, die auch Teil des Schlosses des Chatraumes von Person A ist 15 und somit innerhalb der X% Matchinganforderungen von Person A liegt. Folglich können neben der Person A nur Personen den Chatraum betreten, deren Chatraumschlüssel min X% Übereinstimmung mit dem Chatraumschlüssel von Person A hat. Der Wert X steht für einen Zahlenraum von 0-100.

20

Konkret kann die Benutzung des erfindungsgemäßen Systems folgendermaßen erfolgen:

Der Nutzer - ein Single - entscheidet sich zunächst einmal die Dating-Portal nach 25 der Erfindung zu nutzen, bei der für Singles durch einen auf psychologischer Testtheorie selbstlernenden Algorithmus der perfekt zueinander passende Partner ausgewählt wird (sog. matchen). Dieser selbstlernende Algorithmus wird in Form von Smart Contracts und Oracles auf dem IOTA Tangle Netzwerk aufbauend abgespeichert und alle Daten in Form von Hashes kryptographisch verschlüsselt de- 30 zentral abgespeichert sind.

Bspw. kann in einem Synchronisations-Center die Dateneingabe erfolgen. Hierzu können Synchronisations-Räume (Sync-Raum) vorgesehen sein. Dort können Bildschirm Plätze eingerichtet sein. Der Nutzer legt einen Sensor an den Finger. Auf dem Bildschirm wird der Nutzer aufgefordert, sich mit seiner digitalen Identität, der sogenannten DID (Digital Identity) zu legitimieren. Die DID wird dabei nur kryptographisch in verschlüsselter Form eines sogenannten Hash-Wertes abgespeichert, ebenso wie die vom Nutzer zur Matching-Synchronisation ermittelten physiologischen Daten, bspw. Hautwiderstand und Pulsfrequenz. In Kombination mit der digitalen Identität (DID) und den Optik- und Charakter-Werten ergibt sich dann ein sogenannter Wurzelhash, der sog. persönliche Love-Hash, welcher somit aus dem Hash-Code den erhobenen Matchingdaten besteht, dem sogenannten Love-Seed und der DID. Zur Ermittlung des Profils können bspw. abwechselnd Bilder von jeweils immer 2 Personen nebeneinander gezeigt werden, aus welchen der Nutzer entscheiden soll, wer dem Nutzer optisch besser gefällt. Dabei wertet die Künstliche Intelligenz (KI) zum einen die bewussten Entscheidungen aus und kombiniert diese mit den dabei detektierten körperlichen Reaktionen wie Hautwiderstand, Puls, Pupillenkontraktion und weiteren physiologischen Messdaten. Die Auswertung basiert auf den Erkenntnissen der psychologischen Testtheorie und sogenannten Action Units, also der Erkenntnis, wie bestimmte Mimiken im Gesicht von Psychologen genannt wurden. Diese helfen ein ehrliches Bild von dem zu matchenden Single zu erhalten. Am Ende ermittelt die KI das optische Bild des gewünschten Typs Partner und speichert dieses über die ermittelten Daten in Form eines Hash-Wertes kryptographisch ab. Die Gesichtsmerkmale des gewünschten Partners werden dabei über die entsprechenden Gesichtspunktwerte wie bei der digitalen Gesichtserkennung ermittelt und kryptographisch verschlüsselt abgespeichert. Falls der Nutzer nicht auf das Passfoto der DID zurückgreifen möchte, kann sich der Nutzer bei der Datenerhebung fotografieren lassen, um das Passfoto der DID zu ersetzen. Die KI kann dann später die ermittelten Gesichtspunkte aller in der Datenbank hinterlegten Singles mit den ermittelten Gesichtspunkten des Wunschkandidaten des Nutzers, welche bei ihrer Befragung zu den Bildern erhoben werden, auf min. 80 % Übereinstimmung abgleichen bezüglich

der gegenseitigen optischen Anziehung durch Vergleich der produzierten sog. optischen Wurzelhash-Werte des Nutzers mit denen der potentiellen Kandidaten.

5 Danach erfolgt die Persönlichkeitsbefragung, ein Frage- und Antwort-Algorithmus zur Ermittlung des zum Charakter des Nutzers zu min. 80% passenden Charakters ihres potentiellen Partners. Das so entstandene Anforderungsprofil des Partners sowie das entstandene Persönlichkeitsprofil des Nutzers werden zu dem sogenannten Charakter Wurzel Hash-Wert kombiniert und anschließend mit dem
10 zuvor ermittelten optischen Wurzel Hash-Wert zum finalen Love-Wurzel-Hash kombiniert.

Eine Benachrichtigung über einen Treffer, also ein Match, kann über eine Smartphone App erfolgen, aber auch über ein Matching Armband oder eine Matching Halskette, sog. kryptographischer Schmuck. In der App oder auf dem Schmuck
15 wird zu Beginn angezeigt, wie viele Matches in der Umgebung, bspw. der Stadt oder dem Landkreis, in dem der Nutzer lebt, mit welchem Grad an Übereinstimmung ermittelt wurden. Der Schmuck enthält zudem ein Sensorsystem, mit dem Hautwiderstand, Puls und weitere physiologischen Werte gemessen werden. Über
20 einen Zugang auf die Homepage des Dating Portals kann der Nutzer weitere Informationen abrufen und ggf. Änderungen im Profil vornehmen. Das Einloggen in den gesicherten privaten Bereich kann bspw. durch einen QR-Code der DID erfolgen.

Das Love2Tangle System zeigt auf der Homepage, der App oder dem Schmuck
25 auch an, wie viele potentielle Partner mit welcher Matchingquote an einem Tag dem Nutzer begegnet sind. Treffen zwei Personen mit einer Übereinstimmung von 90% im Herz-Wurzel-Hash aufeinander, wird ein Signal an beide Personen in Form eines einfachen Vibrationsalarms, eines akustischen Signals o. dgl. ausgesandt, wenn der gemessene Hautwiderstand, Puls und die weiteren physiologischen
30 Werte zu min. 90% beim Blickkontakt übereinstimmen. Nur in diesem Fall erfolgt eine Benachrichtigung an beide Personen.