

SYSTEM, METHOD AND DATA COMMUNICATIONS NETWORK FOR CERTIFYING DIGITAL USER ACCOUNTS, PROFILES AND IDENTITIES

FIELD OF THE INVENTION

[0001] The present invention relates to a data communications network and a computer-implemented system and method for certifying digital user accounts, profiles or identities and, in particular, assessing and certifying a user account, profile or identity thereby enabling the user to engage in online transactions using the account, profile or identity across multiple platforms with other users having increased confidence regarding the bona-fides of the user's account, profile or identity as compared with other methods and/or systems.

BACKGROUND OF THE INVENTION

[0002] Online marketplaces, such as Facebook® Marketplace and Gumtree®, which allow shoppers to browse, compare, and purchase items from the comfort of their homes or on-the-go using smartphones, have experienced significant growth and popularity over recent years due to their convenience, diverse product range, competitive pricing, and ease of use. Such platforms foster a sense of community and trust, where buyers and sellers can view each other's profiles, mutual friends, and shared interests, creating a perceived level of trust and security.

[0003] Online marketplaces have expanded their reach into various industries and product categories. Such marketplaces are no longer limited to specific sectors such as e-commerce or electronics, but have diversified to include areas such as fashion, home goods, groceries, services, and more.

[0004] Such marketplaces have also expanded their presence beyond their home countries, with major platforms now operating internationally. This expansion has facilitated cross-border trade and provided opportunities for sellers and buyers from different regions to connect and transact.

[0005] The proliferation of smartphones and mobile apps has also revolutionized online marketplaces. Mobile commerce has experienced significant growth, enabling users to

access and transact in marketplaces anywhere at any time, contributing to the overall growth of these platforms.

[0006] Many online marketplaces operate according to a model that allows third-party sellers to list and sell their products. This has understandably led to an increase in the number of sellers participating in online marketplaces, creating a diverse range of products and fostering competition.

[0007] Over time, online marketplaces have also enhanced trust and confidence amongst consumers with the implementation of buyer protection programs, improved seller verification processes, and offering customer reviews and ratings. These measures have assisted online marketplaces to build credibility and encourage more consumers to shop using online marketplaces.

[0008] Online marketplaces continue to introduce new features and innovations to improve the user experience, including providing personalized recommendations, advanced search capabilities, social sharing, easy payment options, and streamlined checkout processes, all of which have increased user engagement and growth.

[0009] Many online marketplaces have integrated with social media platforms, allowing users to discover and purchase products directly within social media applications (also referred to herein as “apps”). Such integration has further boosted the visibility and expansion of online marketplaces.

[0010] Overall, the growth of online marketplaces over the past five years has been substantially driven by technological advancements, changing consumer preferences, and the convenience and benefits they offer. As these platforms continue to evolve and innovate, further growth and expansion in respect of their use is expected.

[0011] However, a significant problem associated with online marketplaces is the issue of fraud, particularly in relation to online transactions, which is a significant issue that affects both buyers and sellers. Unfortunately, fraudsters take advantage of such platforms to deceive and defraud unsuspecting users who often feel at ease engaging with and sharing information according to a perceived level of security.

[0012] Fraudulent activities on such platforms is effected in various forms. These include, but are not limited to:

- fake products where fraudsters sell counterfeit or misrepresented products (including the use of misleading product descriptions), exploiting the lack of the ability to conduct physical inspections in online transactions;
- non-delivery and tracking number scams where sellers vanish after receiving payment, leaving buyers without their purchased items;
- payment scams where fraudsters trick users into making payments outside the platform, which makes it challenging for buyers to dispute unauthorized charges;
- identity theft involving phishing attempts and scams aimed at stealing personal information, including financial details; and
- use of fake accounts where scammers create fraudulent profiles posing as legitimate sellers, adopt fictitious buyer personas, and manipulate trust through fake reviews and ratings evading detection by frequently changing identities.

[0013] The creation of fake profiles in particular remains an ongoing challenge. As technology advances, the tactics of individuals who establish fake accounts also evolve.

[0014] Fake profiles on social media can take various forms, and are typically created for different purposes. Some common types include:

- “Catfish profiles” which are created by individuals who pretend to be someone else, often using stolen photos and information to deceive others. Catfish profiles may search for personal connections or seeking to engage in scams;
- “Bots” which are automated accounts programmed to perform tasks such as posting spam, spreading misinformation, or artificially inflating follower counts. They can be used for political propaganda, marketing, and other malicious activities;

- “Impersonator Profiles” which are profiles that impersonate a real person, often a celebrity or public figure, to gain followers, spread misinformation, or engage in scams;
- “Seller Profiles” which are profiles created by businesses or individuals to sell products or services. These profiles may use fake information or exaggerated claims to attract customers;
- “Troll Accounts” which are fake profiles created by users to harass or provoke others online. They often engage in offensive behavior, cyberbullying, or hate speech;
- “Clone Accounts” which are duplicate profiles created to mimic real users or organizations, often for the purpose of spreading misinformation, scamming, or phishing;
- “Sockpuppet Accounts” which involve individuals who create multiple profiles to support or defend themselves, their ideas, or their content online, giving the illusion of widespread support or opposition;
- “Ghost Accounts” which are abandoned or inactive profiles that may have been real at a previous point in time but are no longer maintained. They can be used for various purposes, including impersonation or spreading outdated information;
- “Scammer Profiles” which are created with the intention of deceiving others for financial gain. They may engage in romance scams, investment scams, or phishing attempts; and
- “Political Propaganda Profiles” which are used to spread political propaganda or manipulate public opinion. These profiles often “share biased” or include false information to influence elections or public sentiment.

[0015] Such fake profiles exist across various social media platforms, including Facebook®, Instagram®, WhatsApp®, and more. As outlined above, the motivation behind creating fake profiles can vary widely, from spreading misinformation to identity theft and fraud. Some fake profiles borrow information and photos from real users,

creating a believable online persona. This often involves identity theft, where personal images and details are exploited without consent. Other forms of deception rely on automated bots to simulate human interaction. Bots can generate and share content, follow accounts, and engage in conversations enabling them to appear genuine. Sophisticated operators often establish networks of fake profiles which can amplify propaganda, manipulate public opinion, or enable an increased engagement in fraudulent activities.

[0016] There are several challenges associated with combating the creation of fake profiles. For example, those who establish fake profiles often adapt and refine their techniques to avoid detection by algorithms that are created and implemented for the purpose of detecting fake profiles. Further, with billions of users, the administrators of such platforms are required to review an enormous amount of data to identify fake profiles accurately. The volume of accounts means that any attempt(s) to identify false or deceptive accounts is a significant task. A further complication is that detecting and removing fake profiles often causes user privacy concerns.

[0017] Currently, scammers and fraudsters are able to defraud people in online marketplaces due to a combination of factors that exploit vulnerabilities in technology, human psychology, and the anonymity provided by the Internet. The internet allows scammers to hide their true identities, creating a sense of detachment and reducing the risk of any adverse outcome for the scammer. They can operate under fake names, create fake profiles, and use untraceable email addresses or cryptocurrency transactions, making it difficult to track such operators. The internet enables scammers to reach a vast number of potential victims worldwide, and they can target individuals across borders without physical limitations, making it easier to cast a wide net and increase their chances of success. Scammers are also skilled at manipulating human psychology and exploiting trust, and often employ techniques such as impersonation, emotional appeals, urgency, and social validation to deceive and convince victims to divulge sensitive information, send money or allow access to accounts.

[0018] Scammers continually adapt and refine their methods to avoid detection. They use technology tools, including phishing emails, malware, fake websites, and spoofed phone numbers, to deceive people into revealing personal information or engaging in

fraudulent transactions. Many people are unaware of the various scams and fraudulent tactics employed by scammers, and this lack of awareness renders them more susceptible to falling victim to a fraudulent scheme. Additionally, scammers often exploit current events or popular trends such that their scams appear more legitimate and relevant. Scammers often impersonate well-known organizations, financial institutions, government agencies, or familiar individuals to gain trust and credibility. By mimicking reputable brands or trusted individuals, they often deceive victims into providing sensitive information or making financial transactions. The global nature of the internet poses challenges for law enforcement and regulatory bodies. Jurisdictional issues and variations in legal frameworks across different countries make it challenging to investigate and prosecute scammers operating from jurisdictions external to the jurisdiction in which the fraudulent act occurs. Furthermore, scammers are increasingly making use of AI to automate and personalize their fraudulent representations using AI created phishing emails and deepfake technology tools to enhance their prospects of deception and render their schemes more difficult to detect.

[0019] Traditionally, businesses operating in off-line transactions have used documentary Know Your Customer (KYC) procedures to ascertain a person's bona fides to avoid or at least ameliorate some of the abovementioned problems. Such procedures are considered effective for verifying identities in various sectors, and to ensure that any financial malpractice, money laundering scams, terrorism financing, and other unlawful schemes are unable to operate, thus becoming a primary factor with respect to customer identification. It is generally also the first step in the client onboarding process. KYC procedures include ID card verification, face verification, document verification (such as utility bills as proof of address), and biometric verification. Banking institutions must strictly comply with KYC regulations and anti-money laundering regulations to assist government attempts to interrupt and/or disable fraudulent activities. KYC compliance responsibility rests with the banks and any failure of a bank or financial institution to properly implement KYC compliance may result in the bank or financial institution being heavily penalized or cause loss of their banking / financial trading license.

[0020] However, KYC procedures are facing significant challenges due to the proliferation of fake documents. The advent of advanced digital technologies has made it increasingly easier for fraudsters to create convincing counterfeit identification papers.

These fake documents possess sophisticated features that mimic genuine documents, rendering traditional documentary KYC methods less reliable. Consequently, relying solely upon manual document verification is no longer considered safe in relation to combating identity fraud.

[0021] The present invention seeks to mitigate the problems discussed herein, or at least provide an alternative solution to existing systems, methods and data communications network for reducing the incidence of use of falsified digital accounts to mislead and/or deceive others.

[0022] The reference to any prior art in this specification is not, and should not be taken as, an acknowledgement or any suggestion, that the prior art forms part of the common general knowledge.

SUMMARY OF THE INVENTION

[0023] According to one aspect, the present invention provides a computer-implemented method for certifying a user's digital account, profile or identity, the method including, receiving, by one or more processors, details relating to a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions, the request including identification details regarding the user including at least one personal identification parameter, associating, by one or more processors, the user request with an organization account established by the user with an organisation that has observed Know Your Client (KYC) obligations, comparing, by one or more processors, the details relating to the request submitted by the user regarding the digital account, profile or identity, including the user personal identification parameter, with details associated with the organisation account established by the user with the organisation that has observed the KYC obligations, determining, by one or more processors, whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity, and based upon the comparison satisfying the minimum pre-defined certification threshold, certifying, by one or more processors, the user's digital account, profile or identity.

[0024] In an embodiment, the method further includes causing, by one or more processors, regular access regarding the user's digital account, profile or identity, and conducting an updated comparison of same with the details associated with the user's organisation account and, according to an updated comparison satisfying the minimum pre-defined certification threshold, maintaining certification of the user's digital account, profile or identity and in the event an updated comparison fails to satisfy the minimum pre-defined threshold, revoking certification of the user's digital account, profile or identity.

[0025] In an embodiment, the digital account, profile or identity provides the user with the ability to execute and/or arrange transactions or seek certification in respect thereof, wherein the account, profile or identity includes one or more of, an online identity of the user, a social media account or profile of the user (eg. Facebook, Instagram, TikTok, etc), an online marketplace account or profile of the user (eg. Facebook Marketplace), an account of the user associated with an employment site, rental site, certificate validation site, and/or professional validation site, or any other online digital account, profile or

identity that is utilised to execute and/or arrange transactions (eg. financial transactions) and select certification for execution or arranging transactions. As will be appreciated by those skilled in the relevant field of technology, transactions may include purchases, buying and selling, messaging, or any other form of digital interaction and/or communication.

[0026] In an embodiment, the KYC obligations observed by the organisation may include any one or more of, identification card verification, face verification, document verification, or any type of biometric verification including facial recognition. The request including at least one personal identification parameter may include one or more parameters that were used to satisfy KYC obligations. In embodiments of the invention, a range of personal identification parameters are considered including combinations of one or more parameters. In one embodiment, the invention includes parameters such as physical and dimensional biometrics, behavioural biometrics, cognitive biometrics, neuro biometrics, and gesture biometrics. These various biometrics may include behavioural biometrics such as typing speed, rhythm and cadence, pressure applied to keys, time intervals between keystrokes (dwell time) and finger placement and movement during keypresses. Physical and dimensional biometrics may include ear canal shape recognition, vibrational and bone conduction signatures, and/or body odor biometrics, tongue motion tracking, thermal imaging of facial features, skin conductance response (SCR), and vein and capillary pattern recognition. Epigenetic biometrics may also be considered including electromyography (EMG) for muscle activity recognition and bone conduction biometrics. A further biometric measure may include emotional recognition biometrics. There are typically three components associated with KYC processes including a customer identification program (CIP), customer due diligence (CDG) and enhanced due diligence (EDD).

[0027] Accordingly, the solution proposed herein seeks to address, or at least ameliorate problems associated with digital transactions, including identity theft, fake products, non-delivery scams, payment scams, and the use of fake, misleading or deceptive digital accounts used by scammers, by associating or linking a user's digital account, profile or identity (eg. a social media or online marketplace account) with an account previously established by the user with an organisation that has observed the KYC obligations (eg. a bank or financial institution). By comparing details associated with the digital account,

profile or identity and the account established with an organisation that has observed KYC obligations, the bona fides of the user operating the digital account, their profile or identity may be assessed and certified and these steps reduce the instance of fraudulent digital accounts being established and/or maintained by users seeking to engage in misleading, deceptive and/or fraudulent activities.

[0028] In an embodiment, where the user's digital account, profile or identity is certified, the method further includes authorizing, by one or more processors, use of the digital account, profile or identity to execute or arrange transactions.

[0029] In an embodiment, transactions arranged and/or executed by the user may include purchases of goods and/or services (eg. where the digital account is an online marketplace) for which the user authorizes the release of funds from one or more financial accounts associated with the user, with the release of such funds to an intended recipient (eg. seller) only occurring when the seller's digital account, profile or identity is certified. This applies to Business to Consumer (B2C) transactions as well as Peer to Peer (P2P) marketplaces where users buy and sell goods and services directly with each other further necessitating the requirement to certify the identity of the other party before releasing funds.

[0030] In this embodiment, the platform may interoperate with the user's certified digital account, profile or identity (eg. online marketplace or social media account or profile) to enable transactions using the issued electronic card or digital wallet. The platform may also interoperate with the financial institution account of the user, or one or more financial transaction accounts operated by computer implemented systems hosted by financial institutions associated with the user. In one example, a user who has received an electronic card or digital wallet may utilise same to purchase assets (eg. goods and/or services) from a seller in an online marketplace, wherein the platform enables funds to be released to the seller only once the user has confirmed receipt and verified the bona fides of the asset purchased.

[0031] Accordingly, it will be appreciated that when transactions include at least one financial transaction, the method may further include, retaining required funds in escrow, by one or more processors, where the funds include those funds requested to be transferred from the user to the intended recipient in exchange for goods and/or services,

and releasing, by one or more processors, the funds to a financial account nominated by the intended recipient once the financial transaction is approved by the user and the intended recipient and further, based upon the user confirming valid receipt of the goods and/or services. The user associated with the digital account may be the purchaser (eg. when the user is making a purchase from a third party) or the seller (eg. when the user is selling an asset to a third party).

[0032] In an embodiment, if a financial transaction is not approved by the user and the intended recipient of funds, and/or the user has not confirmed valid receipt of the goods and/or services within a predetermined time period, the user and the intended recipient of funds are directed to a third party dispute resolution service.

[0033] In an embodiment, the method further includes, based on required transactions possibly including financial transactions (eg. when the digital account relates to an online marketplace for buying and selling goods and services), issuing, by one or more processors, an electronic card or digital wallet to the user whose digital account, profile or identity has been determined to achieve a minimum certification threshold, the electronic card or digital wallet linked to one or more financial accounts associated with the user and thereby enabling the user to utilise the card or wallet (representing a digital financial account) when completing financial transactions whilst operating the certified digital account, profile or identity.

[0034] In an embodiment, the method further includes implementing, by one or more processors, certification of one or more of the user, the account, profile or identity or any user transactions, wherein the certification includes one or more of multi-modal biometric verification of the user according to one or more of facial biometrics, behavioral biometrics, fingerprint biometrics, palm biometrics, palm vein biometrics, voice biometrics, iris biometrics, and/or DNA and cardio biometrics, Quantum Secured Digital Signatures (QSDS) that enable transactions and certifications to be cryptographically protected against quantum computing threats, and Artificial Intelligence (AI) and Machine Learning (ML) models to continuously monitor the certification of users.

[0035] In an embodiment, the multi-modal biometric assessment includes comparing, by one or more processors, one or more elements of biometric data recorded for the user with any corresponding biometric data obtained and recorded in respect of the user's

organisation account that complies with KYC obligations. In embodiments, biometric and behavioural analysis systems may be used to detect AI-generated deepfakes and malicious actors in real-time. This may include the use of facial micro-movement detection to identify inconsistencies in natural human expressions, lip-sync analysis to detect anomalies between spoken words and lip movements, and eye-tracking technology to monitor unnatural blinking rates and gaze behaviours. Voice biometric analysis may be used to detect anomalies in speech cadence, tonal variations, and response latency that may be indicative of AI-generated voices. Additionally, behavioural biometrics, such as interaction patterns and keystroke dynamics, may identify unnatural pauses, overly fluid or gregarious gestures, or delayed responses in real-time conversations. Embodiments may also employ remote photoplethysmography (rPPG) to detect real-time heart rate and blood flow variations, which AI-generated visuals currently struggle to accurately replicate. These combined biometrics may be incorporated in an attempt to improve detection of deepfake content and malicious actors, enhancing the security and integrity of digital interactions according to the present invention.

[0036] In an embodiment, the method further includes comparing the user's biometrics used in the multi-modal biometric verification of the user with biometrics associated with a new request seeking certification in respect of a digital account, profile or identity, and based on the compared biometrics satisfying a minimum similarity threshold, identifying that the request seeking certification in respect of the digital account, profile or identity is a request that has been initiated by the user.

[0037] In an embodiment, the method further includes, based on detecting that the request seeking certification in respect of the digital account has not been initiated by the user, initiating one or more of denying the new request seeking certification in respect of the digital account, profile or identity and notifying the bona fide user regarding same, blocking the initiator of the new request from future certification, temporarily preventing access to the digital account, profile or identity of the user until such time that the new request seeking certification in respect of a digital account, profile or identity has been fully addressed, and temporarily revoking certification of the digital account, profile or identity of the bona fide user, thereby preventing access to the digital account, profile or identity until such time that an updated comparison satisfying the minimum threshold

requirements to maintain certification of the user's digital account, profile or identity has been completed. In another embodiment, the minimum pre-defined threshold required to certify a user's digital account, profile or identity may be adjusted in accordance with the presence, or absence, of suspicious circumstances and hence, the minimum pre-defined threshold may differ according to the user digital account, profile or identity and any circumstances surrounding the particular digital account, profile or identity. In one particular embodiment, the user may select a minimum pre-defined threshold greater than the threshold selected according to the present circumstances associated with the user's account, profile or identity thereby affording individual user's with the ability to increase the pre-defined threshold to accord with their preference regarding the minimum threshold to be applied.

[0038] In an embodiment, the functions described above are performed by one or more separate and/or coordinated systems.

[0039] In an embodiment, the data communications network, computer implemented method and / or system further includes, generating, according to an outcome of the certification assessment, a score representing the confidence regarding the user's identification, and using the generated score as a further basis upon which to determine whether the user's digital account, profile or identity should be certified.

[0040] In an embodiment, the regularity of accessing and/or downloading data regarding the user's digital account, profile or identity, and conducting an updated comparison of the downloaded data with the details associated with the user's organisation account accords with a selection by the user and/or the organisation regarding a preferred frequency for repeated updated certification of the user's digital account, profile or identity. In a particular embodiment, the regularity is daily (ie. every 24 hours) but may accord with any other schedule according to the user's preference including an update each and every time a transaction is requested irrespective of the period of time between transactions.

[0041] In an embodiment, the organisation which has observed the Know Your Client (KYC) obligations includes one or more of a financial institution (eg. bank), electoral commission, passport register, or driver's licence registry.

[0042] In an embodiment, the digital account, profile or identity is a social media account or profile of the user, and the organization account is an account established with a financial institution of the user that has observed KYC obligations, wherein the user is prompted by the financial institution to certify the social media account or profile by linking the social media account or profile with the account established with the financial institution. Further, a Quantum Secured Digital Unique ID (QSDUID) or other secured digital Unique ID may be integrated into the social media account or profile, the QSDUID using one or more quantum and/or blockchain encryption techniques to cryptographically secure the social media account or profile.

[0043] In an embodiment, the digital account, profile or identity is a social media account of the user, and the organization account is an account established with a financial institution of the user that has observed KYC obligations, wherein the user is prompted by the social media account provider to certify the social media account by linking the social media account with the account established with the financial institution. Further, a Quantum Secured Digital Unique ID (QSDUID) may be integrated into the social media account or profile, the QSDUID using one or more quantum and/or blockchain encryption techniques to cryptographically secure the social media account or profile.

[0044] According to a further aspect, the present invention provides a computer-implemented system for certifying a user's digital account, profile or identity, the system including one or more computer processors configured to receive details relating to a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions, the request including identification details regarding the user including at least one personal identification parameter of the user, associate the user request with an organization account established by the user with an organization that has observed Know Your Client (KYC) obligations, compare the details relating to the request submitted by the user regarding the digital account, profile or identity including the user personal identification parameter, with details associated with the account established by the user with the organisation that has observed the KYC obligations, determining whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity, and based on the comparison satisfying the minimum pre-defined threshold, certifying the user's digital account, profile or identity.

[0045] According to a still further aspect, the present invention provides a non-transitory computer-readable medium including computer instruction code that, when executed on a computer, causes one or more processors to perform the steps of, receiving details of a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions, the request including identification details regarding the user including at least one personal identification parameter of the user, associating the user request with an organization account established by the user with an organisation that has observed Know Your Client (KYC) obligations, comparing the details of the request submitted by the user regarding the digital account, including user personal identification parameter, with details associated with the account established by the user with the organisation that has observed the KYC obligations, determining whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity, and based on the comparison satisfying the minimum pre-defined threshold, certifying the user's digital account, profile or identity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0046] Embodiments of the invention will now be described in further detail with reference to the accompanying Figures in which:

[0047] Figures 1A-1B illustrate, in accordance with an embodiment of the present invention, an exemplary flow diagram of a process that enables a user to seek certification in respect of a digital account, profile or identity;

[0048] Figures 2A-2B illustrate, in accordance with an embodiment of the present invention, an exemplary flow diagram of a process that enables a user to utilise a financial transaction account established during certification of their digital account, profile or identity to pay/receive funds for online marketplace purchases;

[0049] Figure 3 illustrates, in accordance with a further embodiment of the present invention, an exemplary flow diagram of a process that enables a financial institution to offer the service of certifying a customer's digital account in the form of a social media profile; and

[0050] Figure 4 illustrates, in accordance with a still further embodiment of the present invention, an exemplary flow diagram of a process that enables a social media platform to offer certification of each user's social media profile by inviting users to link their profile to a financial account that was created by an organization compliant with KYC obligations.

DETAILED DESCRIPTION OF EMBODIMENT(S) OF THE INVENTION

[0051] For simplicity and illustrative purposes, the present disclosure is described by referring to embodiment(s) thereof. In the following description, numerous specific details are set forth to provide a better understanding of the present disclosure. It will be apparent, however, that the current disclosure may be practiced without limitation to the specific details. In other instances, some features have not been described in detail to avoid obscuring the present disclosure.

[0052] According to an embodiment, the present invention relates to a computer-implemented system and method for certifying (10/290/320/400) a digital account, profile or identity (eg. an online marketplace or social media account) of a user (15/250) to enable the user (15/250) to use their account, profile or identity to execute and/or arrange transactions (20) using the account, profile or identity (eg. financial transactions including buying/selling assets). The system may utilise a central server (25) that facilitates secure communication between the server (25) and data networks communication devices (not depicted in the Figures) associated with users (15), as well as between the user devices themselves, and ensures data synchronization across transactions. Each data communication device may operate a software application that enables users to access the system and method and perform steps necessary to certify their digital account(s), profile(s) or identity.

[0053] It will be apparent to the person skilled in the relevant field of technology that the software application may be a mobile application or a web application operating in a data communications device that is operably connected to a data communications network, and similarly, data communication devices utilised by users may be portable devices or fixed location computer devices. Examples of portable devices include smartphones, computer tablets, smart watches, smart glasses and wearables, whilst examples of fixed location computing devices include dedicated workstations and personal computers.

[0054] Each of Figures 1 and 2 extend over the first two pages (1/5 and 2/5) of the accompanying Figures in order to ensure the features of these flow charts are clearly visible. Accordingly, the portion of Figure 1 on page 1/5 is labelled Fig. 1A whilst the portion of Figure 1 that extends into page 2/5 is labelled Fig. 1B. Likewise, Figure 2

extends over pages 1/5 and 2/5 with the portion of Figure 2 on page 1/5 labelled Fig. 2A and the portion of Figure 2 that extends into page 2/5 labelled Fig. 2B. So that the reader can appreciate how the flow charts of Figure 1 connect with those of Figure 2, symbols *, ** and *** are utilized to identify connecting paths.

[0055] Figures 1A-1B illustrate an exemplary process where a user (15) seeks certification (10) for a digital account, profile or identity, and Figures 2A-2B illustrate an exemplary process in which the digital account of Figures 1A-1B which has been certified enables the user (25) to use their certified account, profile or identity to engage in financial transactions (eg. engaging in e-commerce including buying/selling (20), etc). However, it is to be understood that the process shown in the flow diagram of Figure 1 could equally apply to non-financial accounts, including for example those used for social media platforms. The present invention is not intended to be limited to any one particular type of digital account.

[0056] The term “user account” is used throughout this specification, however, it should be understood that this term is intended to also include within its scope a digital profile or a digital identity of the user.

[0057] The server (25) may include one or more processors and/or databases for handling requests (30) from users seeking to certify their digital accounts for various types of transactions, including but not limited to social media platforms, online marketplaces, and professional validation services. In this regard, the server may receive details relating to a request (30) submitted by or on behalf of a user regarding a digital account from which the user proposes to effect transactions (20). The user's digital account may include one or more of a social media account (eg. Facebook, Instagram, TikTok, etc), an online marketplace account (eg. Facebook Marketplace), an employment site, a rental site, a certificate validation site, a professional validation site, or any other online digital account from which the user has the ability to execute and/or arrange transactions (eg. financial transactions) and prefers/requires certification for execution or arranging of transactions.

[0058] The request includes identification details regarding the user, such as a facial image, and links to an account with an organization (also referred to herein as the “organisation account” not depicted in the Figures) that adheres to Know Your Client (KYC) obligations. This organisation could include a financial institution, electoral commission, or government database, which already holds validated user details. For example, the user will have validated identification details stored by one or more external organisations with whom the user also has an established account. On that basis, one or more of such organisations will have already validated the identification of the user in accordance with KYC obligations, and associating the received user request (30) with one or more of those previously established organisation accounts facilitates certification of the user’s digital account by the system, method and data communications network described herein.

[0059] In this regard, the details relating to the request (30) submitted by the user regarding the digital account, including the user identification details, are compared with details associated with the account established by the user with the pre-existing organisation that followed KYC obligations. In this way, a determination can be made regarding whether the comparison satisfies a minimum certification threshold. Based on the comparison satisfying the minimum threshold, the user’s digital account as operated by the user is certified as shown in step (10) of Figure 1B. The server may subsequently cause a regular download of data from the user’s digital account and conduct a regular fresh comparison of the downloaded data with the details associated with the user’s organisation account and based on each updated comparison satisfying the minimum threshold, the certification of the user’s digital account is maintained. In the event the comparison fails to satisfy the minimum threshold, the certification of the user’s digital account may be revoked.

[0060] In the embodiment shown in Figures 1A-1B, there are a number of additional steps that may be performed between receiving details relating to the request (30) submitted by the user and the comparison of relevant data as described above and eventual certification (10) of the user’s digital account. For example, after submitting the request (30), in steps (40) and (50), the user may be requested to undergo an initial sign up process (eg. utilizing the features of known platforms such as Wordpress® and/or

Bubble iO®) before being prompted at step (60) to select between a manual Sign Up (Manual SU) and a Social Media Sign Up (Socials SU).

[0061] Manual SU requires the user to provide extensive personal details for validation, often through known providers such as ConnectID® (80). Accordingly, if the user selects Manual SU there is an additional burden upon the user to provide details in step (70) that satisfy an initial validation process. Socials SU offers a simplified process by linking to an existing validated social media profile. Accordingly, if the user selects Socials SU, then there is a reduced burden on the user since the user's existing social media account details which have already undergone a form of validation are utilized, as shown in step (90), in which the user selects the social media profile to which they prefer to link their profile, step (100), which provides a sign-on page in which the user may be requested to confirm their social media credentials (eg. username and password), and step (110) in which the user may also be requested to accept or add further information.

[0062] Once sign up is complete (ie. upon successful Manual SU or Social SU), the user may be prompted at step (120) to complete one or more additional authentication steps, including (as shown in the example of Figure 1A) two-factor authentication, to enhance security and ensure identity verification. Such authentication steps are known in the relevant field of technology and will not be described in detail herein.

[0063] In a preferred embodiment of the invention, Artificial Intelligence (AI) and Generative AI techniques are utilized to enhance the validation process. These AI techniques may be utilized in respect of one or more of the process steps detailed in the attached Figures for the following purposes:

- Document Verification: Generative AI may be used to verify the authenticity of identity documents including passports, driver's licenses, utility invoices or any other identification document. In this regard, AI techniques can detect fraudulent or manipulated documents by analyzing patterns and visual cues;
- Facial Recognition: AI and Generative AI techniques may assist in facial recognition for identity verification. AI techniques are available that compare a customer's facial features in real-time with their official photo ID to confirm identity;

- Fraud Detection: AI and Generative AI algorithms may analyze transaction data to identify suspicious activities and potential fraud. These techniques assist financial organisations to detect unusual patterns of behavior that assist to identify potentially fraudulent transactions;
- Natural Language Processing (NLP): NLP models, which are a subset of Generative AI techniques, may assist to analyze customer communications including communications using chat box or email correspondence to identify potential compliance issues or unusual language patterns inconsistent with the users established language patterns that may indicate the need to conduct further investigations;
- Risk Assessment: Generative AI may be utilized to analyze a customer's financial history and behavior to assess credit worthiness and credit risk profile which may assist financial organisations to more appropriately assess existing and/or proposed future lending requests by the user;
- Anti-Money Laundering (AML) and Compliance: AI and Generative AI techniques may assist automation of AML processes conducted by financial organisations by continuously monitoring transactions and customer activities and highlighting transactions that may comprise potential money laundering or a transaction that fails to comply with regulatory requirements;
- Data Security: AI and Generative AI techniques may enhance data security by identifying vulnerabilities and potential threats in real-time which may assist any organisation to improve the protection of sensitive customer information that is retained by the organisation.

[0064] Generative AI can also assist in detecting unusual patterns in respect of user behaviour, identifying compliance issues, and monitoring potential money laundering activities.

[0065] As previously described, the request submitted by the user will include identification details regarding the user including at least a facial image of the user. Step (130) of Figure 1B represents a stage at which the user may be prompted to add biometric information including a facial image. Additional biometrics that a user may prefer, or be prompted, to add at this or another stage of the request/certification process. Additional biometrics may include, but are not limited to, fingerprint biometrics, palm biometrics, palm vein biometrics, voice biometrics, iris biometrics, and/or DNA and cardio biometrics.

[0066] Whilst not depicted in any one particular step of Figures 1A-1B, the user may be prompted to select a particular digital account with which to associate the request (30). Step (140) of Figure 1B represents the stage at which the details relating to the request submitted by the user regarding the digital account, including the user identification details, are compared with details associated with the account established by the user with the organization that has observed the KYC obligations.

[0067] It will be appreciated that a similar process may be performed subsequent to the initial certification step, namely, when causing a regular download of data from the user's digital account and conducting a regular updated comparison of the downloaded data with the details associated with the user's organisation account. The regularity of downloading data from the user's digital account and conducting an updated comparison of the downloaded data with the details associated with the user's organisation account may accord with a selection by the user and/or a selection by the organisation regarding a preferred frequency for certification of a user's digital account, profile or identity. For example, the regularity may be hourly, daily or weekly depending upon the particular requirements and/or preferences of the users and organisations involved.

[0068] Based on certification of the user's digital account, and continued regular maintenance of the certification, the user will be authorized to access their digital account including to execute and/or arrange transactions. One or more additional actions may be performed based upon certification of the digital account, including but not limited to the establishment of a transaction account for the user, which may include issuance/receipt of an electronic transaction card (150) as described in greater detail further below with

reference to Figure 2A, or a digital wallet as described in greater detail further below with reference to Figure 3.

[0069] As described earlier, a user may elect, or be prompted, to provide additional biometric information. Accordingly, in addition to requiring the comparison between details relating to the request submitted by the user regarding the digital account with details associated with the account established by the user with the organisation that has observed the KYC obligations to satisfy a minimum threshold, certification of the digital account operated by the user may further require the user to undergo biometric assessment. For example, one or more elements of biometric data recorded for the user may be compared with any corresponding biometric data obtained and recorded in respect of the user's organisation account. In this regard, a score may be generated that represents the user's identification, wherein generation of the score includes combining and assessing the one or more elements of biometric data recorded for the user. Whilst not shown in step (140) of Figure 1B, the generated score may be used as a further basis for identification comparison to determine certification or otherwise of the user's digital account.

[0070] In order to reduce the incidence of fake or fraudulent accounts (also known as "ghost accounts") being created and attempting certification, additional steps may be implemented. Whilst not shown in Figures 1A-1B, in addition to regularly comparing downloaded data with the details associated with the user's organisation account, the system may compare the user's biometrics used in the biometric assessment of the user with biometrics associated with any new request seeking certification in respect of the digital account. Based upon the compared biometrics satisfying a minimum similarity threshold, the system may identify that the new request seeking certification in respect of a digital account is not a request initiated by a previously certified user who has matching biometrics. The above-described additional steps may be implemented in relation to requests for seeking certification in respect of an existing digital account or may also be used in relation to any request to establish and/or use a digital account, profile or identity.

[0071] Based upon detecting that the new request seeking certification in respect of the digital account has not been initiated by the previously certified user, one or more

corrective and/or preventative actions may be performed. For example, the new request seeking certification in respect of the digital account may be denied and the previously certified user may be notified regarding the attempted establishment of a ghost account. Further, the initiator of the new request may be blocked from further use of the system and their details may be forwarded to a relevant authority. Access to the certified digital account of the user may be temporarily frozen until such time that the new request seeking certification in respect of the digital account has been fully investigated and resolved. Further, certification of the digital account of the user may be temporarily revoked, thereby preventing access to the certified digital account until such time that an updated comparison satisfying the minimum threshold to enable the user to maintain certification of the digital account has been completed. These represent some of potentially many additional actions that could be performed in such circumstances.

[0072] Figures 2A-2B illustrate a particular embodiment in which an electronic card (150) is issued to, and received by, a user who has completed the certification steps detailed in Figures 1A-1B and who subsequently utilizes the electronic card (in combination with the linked transaction account (155) established for the user) to buy/sell goods and/or services in an online marketplace (representing an example of a user digital account in respect of which financial transactions (20) are executed). Step (160) shown in Figure 2A represents an initial authentication step prompting the user to sign in using facial biometrics which enables the user to access the online marketplace to buy/sell goods and/or services as shown in subsequent step (20). Step (170) also allows the user to select an alternative path of inviting new users (step (180)) to be certified, which enables an invitation to be sent to the selected new users to engage with the certification process of Figures 1A-1B, as reflected in step (190).

[0073] The transaction accounts (155) established for users effectively provide an account controlled by an administrator of the system, into which funds may be deposited by the user or by another individual or organization with whom the user is conducting a financial transaction using their certified digital account. In this regard, the user may elect to link a personal banking account established with a financial institution of the user to the transaction account (155) such that funds are transferrable there between. Any funds

deposited into the transaction account (155) are held in escrow by the administrator until such time that certain additional steps are completed, as described below.

[0074] In an example in which the user is buying goods from another individual or organisation (who may or may not have achieved certification of their digital account), the user (purchaser) is invited at step (200) to deposit funds required to complete the purchase from their personal banking account into the transaction account (155). In step (210), the user (purchaser) confirms with the seller their intention to purchase the goods and the transfer of funds into the transaction account (155). The funds are subsequently held in escrow in the transaction account (155) until such time that the user (purchaser) has received the purchased goods as shown in step (220), and subsequent to confirming receipt of the goods, the funds held in the transaction account (155) are released to the seller (ie. only once the user has confirmed receipt and verified the bona fides of the asset purchased), as shown in step (230).

[0075] Accordingly, it will be appreciated that when the transactions (20) undertaken using the certified digital account include financial transactions, any funds requested to be transferred from a purchaser to a seller in exchange for goods and/or services are held in escrow. It is to be understood that the user associated with the certified digital account may be the purchaser (eg. when the user is making a purchase from a third party using the certified digital account as described above with reference to Figures 2A-2B) or the seller (eg. when the user is selling an asset to a third party using the certified digital account).

[0076] In circumstances where the financial transaction is not validated by the purchaser and the seller, and/or the purchaser has not confirmed receipt of the goods and/or services within a predetermined time period, the purchaser and seller may be invited to resolve any issues to enable the release of funds, failing which, the funds will remain in the transaction account (155). In the event that resolution cannot be reached, the purchaser and seller may be directed to a third party dispute resolution service.

[0077] Figure 3 illustrates a further embodiment in which a financial institution (240), such as a bank (or payment service provider or financial institution), contacts its

customers (250) and offers the service of certifying the customer's social media profile using the bank's (or payment service provider's or financial institution's) existing KYC data. The certification process may be facilitated through an orchestration platform which utilises the bank's previously validated data to securely and efficiently certify the social media account.

[0078] It will be appreciated that the present invention is not limited to only banks initiating the certification process as described above. For example, in an alternative embodiment, social media platforms themselves may contact their users to commence the identity certification process, as described in greater detail below with reference to Figure 4. In this scenario, the social media company, utilising its existing relationship with the user may, invite them to link their social media profile with a bank or Payment Service Provider (PSP) account for certification. This method allows social media platforms to take proactive steps to enhance the authenticity of their user base, offering certified profiles as a value-added feature that increases community user trust and engagement.

[0079] In the embodiment shown in Figure 3, the bank (240) first initiates (260) the social media profile certification by identifying eligible customers. These customers would typically have already undergone KYC verification as part of the bank's (240) regulatory compliance processes. This existing KYC data includes verified personal information, such as identity documents, facial images, residential address, and financial history. Once eligible customers are identified, the bank (240) may send a notification or invitation (eg. through the customer's (250) banking app or via email), offering them the opportunity to certify their social media profiles using the bank's secure KYC system.

[0080] Upon receiving notification, the customer (250) is prompted to accept (270) the invitation and log into the bank's (240) digital platform (eg. through a mobile banking app or via a secure web portal). The customer (250) is then guided through a consent form, agreeing to allow the bank (240) to access their social media profile and to link (280) same with their KYC data. This process ensures that both privacy and security standards are maintained.

[0081] The customer's social media profile data may be retrieved by searching the unique social media identifier, requesting login credentials or utilizing customer authorization from the social media platform. Once acquired, the system may obtain relevant data, such as profile photos, username, email address and other identifying details from the social media account. This data is compared with the KYC information already obtained and held by the bank to certify (290) the identity of the social media account holder (250).

[0082] The entire process, from the customer's initial consent (270) to the final certification (320), may utilize a comprehensive suite of advanced assessment measures. These measures may include multi-factor authentication, end-to-end encryption, and Secure Socket Layer (SSL) protocols. The system may also integrate Quantum Secured Digital Signatures (QSDS), as described in greater detail below, to ensure that every transaction and certification is cryptographically protected against both current and future quantum computing threats. Additionally, the system may employ multi-modal biometric verification techniques, such as facial recognition, voice analysis, fingerprint scanning, and behavioral biometrics, to authenticate users with a high degree of accuracy and security. Artificial Intelligence (AI) and Machine Learning (ML) models may continuously monitor the certification process and user behavior in attempt to detect and minimise fraudulent activities in real-time.

[0083] Such models may analyze patterns and anomalies to flag suspicious actions, enhancing the efficacy and efficiency of the certification process. Furthermore, advanced risk assessment algorithms may evaluate each interaction, dynamically adjusting security protocols to ensure compliance with territory regulatory standards such as GDPR and AML.

[0084] As shown in Figure 3, the bank (240) may, at the request of the social media profile owner (250), integrate a Quantum Secured Digital Unique ID (QSDUID) into the customer's social media profile. This ID is generated (300) using quantum and/or blockchain encryption techniques and may be attached (310) to the customer's certified social media profile.

[0085] Alternatively, the social media platform may initiate the integration of the QSDUID by contacting users directly. This approach enables the platform to offer a seamless and user-friendly experience, where the certification process is streamlined through the social media platform's interface. Users (250) may be invited to connect their bank or PSP accounts to certify their identity and attach the QSDUID to their profiles. This not only simplifies the process for the user (250) but also allows social media companies to establish a higher level of trust within their ecosystems, making them more attractive to users (250) and advertisers alike.

[0086] In a particular example, the process may begin when a bank (240) or PSP, after certifying (290) the customer's identity using their existing KYC data, generates (300) a unique quantum-secured identifier. The QSDUID may then be permanently linked (310) to the customer's social media profile. This attachment ensures that the social media profile is cryptographically secured, and any modification or tampering of the profile will invalidate the quantum signature which may trigger security alerts.

[0087] Once the social media profile has been certified (320) against the KYC data and has a QSDUID linked (310) thereto, the system may proceed to link (320) the certified social media profile with the customer's (250) bank account. This linkage enables the social media profile to become an officially recognized part of the customer's (250) digital identity within the bank's (240) ecosystem. In parallel, a digital certification badge may be created, confirming that the social media profile is now certified according to the bank's (240) KYC process.

[0088] The social media profile, once linked the QSDUID, therefore becomes a digital asset that is cryptographically secured. Any future interactions, modifications, or transactions (330) conducted using this profile can only be validated by use of this quantum-secured identifier. This creates a permanent, secure link between the profile and the verified customer. By linking (310) the social media profile with a quantum-secured ID, the profile is protected against identity theft, impersonation, or account takeovers. Any unauthorized attempts to access or alter the profile will result in the quantum signature being invalidated. For marketplaces and digital platforms, the QSDUID establishes a higher level of trust between parties. Buyers and sellers can be

confident that they are dealing with profiles that are linked to verified bank or PSP customer accounts.

[0089] Once the QSDUID is attached (310) to a profile, the security link between the customer's (250) social media presence and their bank (240) or PSP may remain in place indefinitely. This ensures that even as social media platforms evolve or as the customer (250) moves between platforms, the quantum-secured identity remains valid and recognized across all digital marketplaces.

[0090] The integration of QSDUID into social media profiles also enables enhanced transaction security. Any financial transactions (330) conducted through digital platforms using the pending payment escrow facility may be validated using the QSDUID, providing a link between the buyer's and seller's certified identities. This reduces transaction risk, particularly in peer-to-peer marketplaces like Facebook Marketplace, and other classified platforms where fraudulent profiles are presently a persistent issue.

[0091] By linking social media profiles with quantum-secured certified identities, users may engage in the digital economy with increased confidence regarding the bona fides of digital account, profile or identity with whom they are engaging digitally.

[0092] The QSDUID can also serve as the basis for future multi-platform verification systems, where users (250) with a QSDUID can seamlessly authenticate themselves across various social media platforms and marketplaces without the need for repetitive KYC processes. The ID will preferably be universally recognized by all participating platforms, enabling secure, cross-platform identity certification and transaction validation.

[0093] Certified social media profiles, secured by QSDUID and quantum technologies, may be used as a trusted identity across various digital and physical domains, from online transactions to real-world access control systems. This positions social media platforms to not only enhance their security offerings but also to offer digital identity-as-a-service to third-party providers.

[0094] The system may also integrate a digital wallet functionality as part of the customer's (250) bank account. This digital wallet may be used for peer-to-peer payments, online shopping, and other transactions linked to the customer's (250) certified social media profile. The digital wallet may be seamlessly integrated with the bank's (240) mobile app and online banking portal, providing the user (250) with easy access to manage their social media-linked transactions.

[0095] The bank (240) may also offer additional services (340) following social media certification. For instance, the customer (250) may use their certified social media profile as an authentication method for third-party services, such as e-commerce platforms and peer-to-peer marketplaces. This multi-platform verification process may be enabled by an orchestration platform, which securely shares certification data with third-party services, ensuring compliance with territory regulatory standards such as General Data Protection Regulation (GDPR) and Advanced Mobile Location (AML). Furthermore, the certified profile may be used for digital identity certification across other industries, such as healthcare for accessing telemedicine services, education for student enrollment and alumni verification, and real estate for tenant screening and rental agreements.

[0096] Loyalty programs may also be enabled (eg. in the hospitality and travel sectors) by linking customer identities to rewards and benefits. For employers, the certified social media profile could provide a means to verify employee credentials or monitor adherence to corporate policies, particularly in regulated industries such as finance or law enforcement. The versatility of the orchestration platform may also allow it to support "use cases" where identity assurance and trust are important thereby, providing a scalable and secure solution for cross-industry adoption.

[0097] As previously described, the system may allow certifications to be automatically revoked according to the described comparison data no longer satisfying a minimum threshold. In the context of the embodiment shown in Figure 3, the orchestration platform may allow continuous monitoring of the customer's (250) social media profile and their bank account. Any significant changes to the customer's (250) social media account, such as a change in username, profile picture, or other key identity markers, may trigger a re-

certification process, ensuring that the certified social media profile remains accurate and up-to-date.

[0098] Customers (250) may also be provided with the ability to revoke the certification at any time. In the embodiment of Figure 3, this revocation may be handled through the bank's (240) platform or any third party platform, where the customer (250) can remove their social media profile from their bank account. Upon revocation, the system may promptly delete the associated data and notify any linked third-party services that the certification has been withdrawn.

[0099] The bank (240) or any third party platform may offer a tiered certification system. This system allows customers (250) to select different levels of certification depending upon their needs. For instance, a basic certification might involve verifying the name and email address associated with the social media profile, while an advanced certification might include biometric verification through facial recognition, using the customer's (250) bank-registered biometric data. This may be extended to other financial institutions and service providers, such as credit unions, payment service providers (PSPs), and digital wallets. These institutions may adopt the same orchestration platform to offer social media profile certification services to their customers.

[0100] The system's architecture may be configured for scalability, allowing integration of multiple social media platforms and third-party service providers. As social media continues to evolve, the orchestration platform should remain flexible, able to accommodate new platforms and verification methods, including emerging trends such as decentralized identities and blockchain-based social networks.

[0101] Once the certification (290) of a customer (250) has been completed, including the certification of the customer's (250) social media profile and integration of the digital wallet, the certified bank customer (250) is able to utilize the digital wallet across various digital marketplaces. This includes the ability to buy and sell goods and services using the pending payment escrow facility, as previously described.

[0102] The escrow facility ensures that funds are held by the financial institution (240) while the transaction between the buyer and seller is pending. The system therefore acts as a trusted intermediary, guaranteeing that the buyer's payment is only released once the agreed conditions of the sale have been met, such as the delivery of goods or services. This process may be fully automated, utilising the orchestration platform to manage the entire escrow lifecycle, from the initiation of a transaction to its final settlement. Accordingly, the digital wallet's escrow functionality adds an additional layer of security for both buyers and sellers, reducing fraud and increasing trust within digital marketplaces. The escrow service is particularly beneficial for high-value transactions or those involving goods and services that require verification upon delivery.

[0103] Notifications and updates may be provided to both parties at each stage of the transaction and escrow process, including confirmation of payment, shipment of goods, and final release of funds. Furthermore, the system may be integrated with various online marketplaces, including e-commerce platforms, peer-to-peer marketplaces, and classified advertisement sites. Once the bank customer (250) has linked (280) their certified social media profile and activated their digital wallet, they can easily engage in transactions across multiple platforms whilst benefiting from the enhanced confidence provided by the escrow system. This system significantly reduces the risk of scams, particularly in high-fraud environments such as social media marketplaces.

[0104] As previously described, the escrow system may also offer a dispute resolution feature, allowing buyers and sellers to resolve any disputes directly within the platform. This embodiment of the invention may be supported by AI-driven fraud detection algorithms, which may monitor transaction behaviors and flag suspicious activity. In instances where disputes arise, the platform may offer a mechanism to hold funds in escrow until a resolution is reached, protecting both parties from potential fraud or disputes. The addition of this escrow functionality extends the usability of the certified digital account, profile or identity beyond social media certification and financial transactions. This embodiment is expected to enhance user trust in digital commerce by offering a secure, bank-verified identity linked to a robust, bank-regulated financial instrument (ie. digital wallet).

[0105] Accordingly, enhancing a secure digital wallet with integrated escrow enables a more comprehensive approach to provide safe and transparent transactions in digital marketplaces. This not only supports individual buyers and sellers but also increases the overall trust in online transactions across a wide array of digital platforms, including social media marketplaces such as Facebook Marketplace, peer-to-peer marketplaces, and auction sites. Embodiments may extend the escrow service to enable cross-border transactions, providing an international escrow functionality that complies with all required jurisdictional financial regulations. The orchestration platform may dynamically adapt to local laws, ensuring seamless international transactions with the same level of security and trust as compared with domestic payments.

[0106] The digital wallet functionality may also allow users (250) to link their certified profiles with a payment method, enabling secure transactions. These wallets may not only store traditional payment data but may also include the user's certified identity through the process.

[0107] Accordingly, the combined use of KYC-supported social media certification, digital wallets, and escrow service provides a substantially improved environment for peer-to-peer transactions.

[0108] After successful certification (320) of social media profiles through the bank's (240) KYC-backed certification process, users (250) may be granted the ability to use this certification across multiple digital platforms. Not only may the certified profiles be linked to the relevant bank account, but as previously described, the integration may also allow for the automatic creation of a digital wallet linked to the customer's certified identity. The certified users, having their identity secured by both the bank's KYC data and the Social Media Identity Securitisation (SMIS) system are able to participate in digital commerce with confidence. Whether they are buying or selling goods on a peer-to-peer marketplace such as Facebook Marketplace, the certified users will be granted a verified transaction status.

[0109] In the context of peer-to-peer marketplaces, the digital wallet may serve as a central point for transactions. Sellers and buyers may transact with full confidence,

knowing that both parties have undergone stringent identity verification and certification of their digital account, profile or identity. The data orchestration ensures that each transaction is linked to certified individuals (250), minimizing the risk of fraud and enhancing transactional transparency. Following the initiation of a transaction, the previously described pending payment escrow facility may be effected.

[0110] Quantum Secured Digital Signatures (QSDS) may also be integrated into the data orchestration framework. As quantum computing continues to evolve, traditional cryptographic methods are increasingly vulnerable to quantum attacks. By utilising QSDS, the integrity and authenticity of data is protected against even the most advanced computational threats.

[0111] Quantum Digital Signatures operate using the principles of quantum mechanics to improve the security of digital signatures in transactions. Unlike classical digital signatures, which rely upon mathematical encryption, quantum signatures exploit the properties of quantum entanglement and superposition. This results in a level of security that is generally considered unbreakable by conventional or quantum computers.

[0112] Within the data orchestration platform, QSDS may play a role in authenticating both the users (250) and the transactions. Each transaction may be assigned a quantum-secured signature, which is unique and cannot be replicated without detection. This prevents unauthorized modifications, ensuring the highest level of integrity for financial transactions, identity verification, and social media profile certifications.

[0113] In a particular example, the process begins when a user (250) initiates a transaction within the banking ecosystem, whether certifying a social media profile or making a purchase using the digital wallet. The system may generate a unique quantum-secured signature for the transaction, which is subsequently verified against the bank's KYC data and the user's quantum key.

[0114] The integration of QSDS further enhances the pending payment escrow facility. Each transaction, from initiation to completion, may be supported by quantum-secured signatures. This means that once the buyer's payment is placed in escrow, the quantum

signatures ensure that the funds are cryptographically locked and can only be released when both parties satisfy the agreed conditions. Any attempt to interfere with, or alter, the transaction may immediately invalidate the quantum signature, alerting the system to potential fraud.

[0115] Incorporating quantum technology into the data orchestration layer according to an embodiment herein not only protects transactions from fraudulent activity provides confidence regarding emerging quantum threats. The use of QSDS creates a tamper-proof, verifiable chain of trust, ensuring that every transaction processed is authenticated at the quantum level.

[0116] Furthermore, Quantum Secured Digital Signatures enable multi-party verification, allowing multiple stakeholders to verify the legitimacy of a transaction without compromising security. In marketplaces where multiple parties may be involved in a transaction, such as buyers, sellers, and third-party escrow services, QSDS ensures that all parties may verify the authenticity of the transaction without risking their own cryptographic keys or data.

[0117] Accordingly, the combination of KYC-backed certification, digital wallets, pending payment escrow, and Quantum Secured Digital Signatures and multi modal biometrics establishes a framework for digital identity certification and transaction management that provides a high level of confidence. This data orchestration ensures that every digital action, whether on social media platforms or in financial markets, is supported by quantum-resistant security, significantly reducing the risk of fraud, identity theft, and data manipulation. By improving the platform with quantum-resistant technologies, the platform is capable of addressing both current and emerging threats in the rapidly evolving digital marketplace ecosystem.

[0118] The orchestration system described herein may be adapted for industries beyond payments, expanding the utility of the quantum-secured identity verification process to sectors such as insurance, finance, human resources and healthcare.

[0119] Accordingly, it will be appreciated that the orchestration platform's flexibility allows various industries to utilise quantum-secured digital identities for enhanced security and personalized services.

[0120] According to the further alternative embodiment shown in Figure 4, the certification process may be initiated by the social media company or platform (350) itself. This proactive approach allows the social media platform (350) to contact its users (250) and offer enhanced security and verification by inviting them to link their profiles to verified financial accounts. This method empowers social media platforms (350) to improve trust among their user base and protect against fake accounts and scams.

[0121] The process begins when the social media platform (350) identifies (360) users (250) for certification and presents the users (250) with an invitation or notification (370) to certify their social media profiles. This invitation may be triggered during a login process, when a user (250) interacts with platform services, or as part of a promotional feature encouraging users to gain certified status. Users (250) may receive (380) and accept the invitation, and subsequently be directed to a secure interface where they may link (390) their social media profile with a bank (240) or PSP account. Upon linking, the platform may use the bank's KYC data to certify (400) the user's identity.

[0122] Accordingly, once the user (250) consents to verification, the platform may securely connect to the user's financial institution (240) to certify (400) their identity using existing KYC data and protocols. Following certification, the platform may generate (410) a Quantum Secured Digital Unique ID (QSDUID), which may be permanently linked to the user's social media profile. This digital ID provides cryptographic certainty that the user's profile will always remain tied to their certified identity, preventing impersonation and fraudulent activities.

[0123] Upon successful certification, the user's profile may be upgraded with a certified badge, indicating that their identity has been certified, thereby enhancing trust between users (250) on the platform. Certified users (250) may also gain access to additional features (420), such as increased visibility, exclusive content, or premium services. For

the social media platform, this reduces the prevalence of fake profiles, bots, and scams, which improves the overall user experience and increases platform credibility.

[0124] This orchestration model may be applied across different types of platforms. For instance, professional networking sites such as LinkedIn may integrate this system to validate user credentials, while e-commerce platforms may use it to certify seller identities. By incorporating (430) certified identities into multiple sectors, platforms can offer increased security and trustworthiness across the digital landscape.

[0125] The QSDUID may also be used to authenticate users across multiple platforms, enabling a seamless and trusted experience. Once a user's identity is certified, they may use the same QSDUID for authentication on other social media platforms, e-commerce websites, and even physical access systems. This multi-platform verification simplifies the user experience by eliminating the need for multiple identity checks, while ensuring robust security across platforms.

[0126] According to the embodiments, the process may employ robust security measures, including Quantum Secured Digital Signatures (QSDS) and multi-modal biometric authentication (such as facial recognition, fingerprint scanning, and voice verification), to protect user data and ensure the authenticity of interactions. Data shared between the social media platform (350) and the financial institution (240) may be encrypted and processed in compliance with global regulations, such as GDPR, AML, and CCPA. Such a configuration provides significant levels of security and privacy for users.

[0127] Once verified, the social media platform may use AI implemented analytics to monitor the behavior of certified users (250) seeking indications of suspicious activity. If the system detects any anomalies, such as attempts to alter the certified profile or engage in fraudulent behavior, it may flag the profile for review or require additional authentication. This monitoring provides an additional layer of fraud reduction, protecting users (250) from scams and harmful interactions.

[0128] The skilled person will appreciate that embodiments of the invention according to the present disclosure provide a solution to problems associated with digital transactions, including identity theft and the use of fake digital accounts by scammers, by associating or linking a user's digital account, profile or identity (eg. a social media or online marketplace account, profile or identity) with an account previously established by the user with an organisation (eg. a bank) that has observed KYC obligations, such that the user's digital account, profile or identity achieves a certified status. By regularly comparing details associated with the digital account with the account established with an organisation that has observed KYC obligations, the bona fide's of the user's digital account, profile or identity may be re-assessed and updated based upon the outcome of the assessment. In other words, the certification can either be maintained or revoked. Further, by controlling or managing financial transactions performed using certified digital accounts, profiles or identities, including holding funds in escrow until such time that both purchaser and seller are satisfied regarding completion of the transaction, there is a reduced likelihood of the incidence of scams such as non-delivery scams, fake products and payment scams.

[0129] Once the process for linking a user's account, profile, or identity to an account previously established with an organization that has observed KYC obligations, the certified account, profile or identity may be used to engage in transactions across multiple platforms, including with respect to use of a pending payment escrow facility. The certified account, profile or identity may be integrated with the user's financial institution or PSP, and in this way, transactions may be facilitated with the use of a secure digital wallet administered by the financial institution or PSP. Such digital wallets may also include integrated escrow functionality. Multi-modal biometric verification, the integration of Quantum Secured Digital Unique IDs, and the use of Quantum Secured Digital Signatures may further enhance security in respect of such transactions.

[0130] It will be appreciated by persons skilled in the relevant field of technology that numerous variations and/or modifications may be made to the invention as detailed in the embodiments without departing from the spirit or scope of the invention as broadly

described. The present embodiments are, therefore, to be considered in all aspects as illustrative and not restrictive.

Throughout this specification and claims which follow, unless the context requires otherwise, the word “comprise”, and variations such as “comprises” and “comprising”, will be understood to imply the inclusion of a stated feature or step, or group of features or steps, but not the exclusion of any other feature or step or group of features or steps.

The claims defining the invention are as follows:

1. A computer-implemented method for certifying a user's digital account, profile or identity, the method including:

receiving, by one or more processors, details relating to a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions;

the request including identification details regarding the user including at least a facial image of the user;

associating, by one or more processors, the user request with an organization account established by the user with an organisation that has observed Know Your Client (KYC) obligations;

comparing, by one or more processors, the details relating to the request submitted by the user regarding the digital account, including user identification details, with details associated with the account established by the user with the organisation that has observed the KYC obligations;

determining, by one or more processors, whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity; and

based on the comparison satisfying the minimum pre-defined threshold, certifying, by one or more processors, the user's digital account, profile or identity.

2. A method according to claim 1, further including:

causing, by one or more processors, regular access to data regarding the user's digital account, profile or identity, and conducting a regular updated comparison of the accessed data with the details associated with the user's organisation account;

based on an updated comparison satisfying the minimum pre-defined certification threshold, maintaining certification of the user's digital account, profile or identity as operated by the user; and

based on an updated comparison failing to satisfy the minimum pre-defined threshold, revoking certification of the user's digital account, profile or identity.

3. A method according to either claim 1 or claim 2, wherein the digital account, profile or identity provides the user with the ability to execute and/or arrange transactions or seek certification in respect thereof, wherein the account, profile or identity includes one or more of:

an online identity of the user,

a social media account or profile of the user,

an online marketplace account or profile of the user,

an account of the user associated with an employment site, rental site, certificate validation site, and/or professional validation site.

4. A method according to any one of the preceding claims, wherein the KYC obligations observed by the organisation include one or more of:

identification card verification,

face verification,

document verification, and

biometric verification.

5. A method according to any one of the preceding claims, further including:

based upon the user's digital account, profile or identity being certified, authorizing, by one or more processors, use of the digital account, profile or identity to execute or arrange transactions.

6. A method according to any one of the preceding claims, wherein the transactions arranged and/or executed by the user include purchases of goods and/or services for which the user authorizes the release of funds from one or more financial accounts

associated with the user, with the release of such funds to an intended recipient only occurring when the user's digital account, profile or identity is certified.

7. A method according to claim 6, further including:

securely holding in escrow, by one or more processors, funds requested to be transferred from the user to the intended recipient in exchange for goods and/or services in a digital account, and

releasing, by one or more processors, the funds to a financial account nominated by the intended recipient based upon the financial transaction being approved by the user and the intended recipient, and further based upon the user confirming valid receipt of the goods and/or services.

8. A method according to claim 7, wherein where the financial transaction is not approved by the user and the intended recipient of funds, and/or the user has not confirmed valid receipt of the goods and/or services within a predetermined time period, directing the user and the intended recipient of funds to a third party dispute resolution service.

9. A method according to any one of claims 5 to 8, further including:

based on the transactions including financial transactions, issuing, by one or more processors, an electronic card or digital wallet to the user whose digital account, profile or identity has been certified, the electronic card or digital wallet linked to one or more financial accounts associated with the user and thereby enabling the user to utilise the card or wallet when completing financial transactions whilst operating the certified digital account, profile or identity.

10. A method according to any one of the preceding claims, further including:

implementing, by one or more processors, verification, authentication and/or security assessments to one or more of the user, the account, profile or identity certifications, and the transactions, wherein the verification, authentication and/or security assessments include one or more of:

multi-modal biometric verification of the user according to one or more of:

facial biometrics,
behavioral biometrics,
fingerprint biometrics,
palm biometrics,
palm vein biometrics,
vein pattern recognition,
hand geometry analysis,
signature recognition,
electroencephalography (EEG) and brainwave patterns,
electrocardiography (ECG) – heartbeat patterns,
olfactory biometrics (body odour analysis),
ear shape recognition,
skin texture analysis,
behavioural biometrics,
body movement patterns (micro-expressions),
genomic biometrics,
voice biometrics,
iris biometrics,
DNA and cardio biometrics,
retinal scanning, and/or

gait recognition,

Quantum Secured Digital Signatures (QSDS) integration to enable transactions and certifications to be cryptographically protected against quantum computing threats, and/or

Artificial Intelligence (AI) and Machine Learning (ML) models to continuously monitor the certification of users.

11. A method according to any one of the preceding claims, further including:

implementing, by one or more processors, verification, authentication and/or security assessments to one or more of the user, the account, profile or identity certifications, and the transactions, wherein the verification, authentication and/or security assessments include one or more of:

behavioural biometric verification of the user according to any one or more of:

typing speed,

rhythm and cadence,

applied key pressure,

dwelling time between key strokes,

Finger placement and movement characteristics.

12. A method according to either claim 10 or claim 11, wherein assessment according to multi-modal biometric data, behavioural biometric data, cognitive biometric data and/or AI implemented continuous authentication and learning enhanced biometric data includes comparing, by one or more processors, one or more elements of corresponding data recorded for the user in respect of the user's organisation account.

13. A method according to any one of claims 10 to 12, further including:

comparing the user's biometrics used in the multi-modal biometric verification of the user with biometrics associated with a new request seeking certification in respect of a digital account, profile or identity, and

based on the compared biometrics satisfying a minimum similarity threshold, identifying that the request seeking certification in respect of the digital account, profile or identity is a request that has been initiated by the user.

14. A method according to claim 13, further including:

based on detecting that the request seeking certification in respect of the digital account has not been initiated by the user, initiating one or more of:

denying the new request seeking certification in respect of the digital account, profile or identity and notifying the user regarding same,

blocking the initiator of the new request from future certification,

temporarily preventing access to the digital account, profile or identity of the user until such time that the new request seeking certification in respect of a digital account, profile or identity has been fully addressed, and

temporarily revoking certification of the digital account, profile or identity of the user, thereby preventing access to the digital account, profile or identity until such time that an updated comparison satisfying the minimum threshold to maintain certification of the user's digital account, profile or identity has been completed.

15. A method according to any one of claims 10 to 14, further including:

generating, based on an outcome of the verification, authentication and/or security assessments, a score representing the user's identification, and using the generated score as a further basis upon which to determine whether the user's digital account, profile or identity should be certified.

16. A method according to any one of the preceding claims, wherein the regularity of downloading data regarding the user's digital account, profile or identity, and conducting

an updated comparison of the downloaded data with the details associated with the user's organisation account accords with a selection by the user and/or the organisation regarding a preferred frequency for certification of the user's digital account, profile or identity.

17. A method according to any one of the preceding claims, wherein the organization which has observed the Know Your Client (KYC) obligations includes one or more of:

- a financial institution;
- electoral commission;
- passport register; or
- driver's licence registry.

18. A method according to any one of the preceding claims, wherein the digital account, profile or identity is a social media account or profile of the user, and the organization account is an account established with a financial institution of the user that has observed KYC obligations, wherein the user is prompted by the financial institution to:

- certify the social media account or profile by linking the social media account or profile with the account established with the financial institution, and

- integrate a Quantum Secured Digital Unique ID (QSDUID) into the social media account or profile, the QSDUID using one or more quantum and/or blockchain encryption techniques to cryptographically secure the social media account or profile.

19. A method according to any one of the preceding claims, wherein the digital account, profile or identity is a social media account of the user, and the organization account is an account established with a financial institution of the user that has observed KYC obligations, wherein the user is prompted by the social media account provider to:

- certify the social media account by linking the social media account with the account established with the financial institution, and

integrate a Quantum Secured Digital Unique ID (QSDUID) into the social media account or profile, the QSDUID using one or more quantum and/or blockchain encryption techniques to cryptographically secure the social media account or profile.

20. A computer-implemented system for certifying a user's digital account, profile or identity, the system including one or more computer processors configured to:

receive details relating to a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions, the request including identification details regarding the user including at least one personal identification parameter of the user;

associate the user request with an organization account established by the user with an organization that has observed Know Your Client (KYC) obligations;

compare the details relating to the request submitted by the user regarding the digital account, profile or identity including the user personal identification parameter with details associated with the account established by the user with the organisation that has observed the KYC obligations;

determine whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity; and

based on the comparison satisfying the minimum pre-defined threshold, certify the user's digital account, profile or identity.

21. A non-transitory computer-readable medium including computer instruction code that, when executed on a computer, causes one or more processors to perform the steps of:

receiving details of a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions, the request including identification details regarding the user including at least a facial image of the user;

associating the user request with an organization account established by the user with an organisation that has observed Know Your Client (KYC) obligations;

comparing the details of the request submitted by the user regarding the digital account, including user identification details, with details associated with the account established by the user with the organisation that has observed the KYC obligations;

determining whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity; and

based on the comparison satisfying the minimum pre-defined threshold, certifying the user's digital account, profile or identity.

22. A data communications network and method of operating same for certifying a user's digital account, profile or identity, the method operated within the data communications network including:

receiving, by one or more processors in an operably connected data communications device, details relating to a request submitted by or on behalf of a user regarding a digital account, profile or identity from which the user proposes to effect transactions;

the request including identification details regarding the user including at least one personal identification parameter of the user;

associating, by one or more processors in an operably connected data communications device, the user request with an organisation account established by the user with an organisation that has observed Know Your Client (KYC) obligations;

comparing, by one or more processors in an operably connected data communications device, the details relating to the request submitted by the user regarding the digital account, including the user personal identification parameter with details associated with the account established by the user with the organisation that has observed the KYC obligations;

determining, by one or more processors in an operably connected data communications device, whether the comparison satisfies a minimum pre-defined threshold to certify the digital account, profile or identity; and

based upon the comparison satisfying the minimum pre-defined threshold, certifying, by one or more processors in an operably connected data communications device, the user's digital account, profile or identity.