is largely commercially developed by market leaders such as IBM and Microsoft, although many smaller companies offer identity and access management solutions.

A study conducted in 2015 estimates that the IAM market will increase from US$8.09 Billion in 2016 to US14.82 Billion by 2021. Major drivers in this area include compliance, process inefficiency and changes in technology trends. Another major driver is the increase in security breaches for global organisations; stolen employee credentials is the largest cause of breach incidents and it is predicted the global business cost will rise to US$2 trillion by 2019 [17]. This is inclusive of cloud-based options such as Identity-as-a-Service (IDaaS).

4.3.2. Identity as a Service. IDaaS refers to Identity and Access Management Services that are offered as part of cloud or Software-as-a-Service subscription-based products. This type of IAM solution contrasts with traditional solutions that operate entirely on-premises, self-managed and delivered through software or hardware means. Largely these solutions rely heavily on existing technology such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

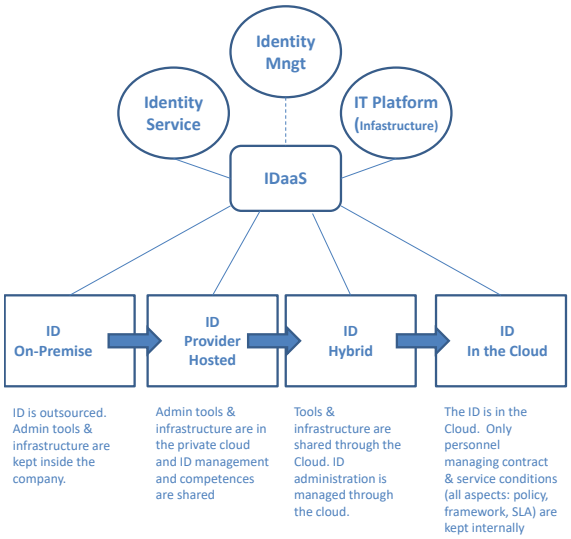

Figure 3. Identity as a Service

This is another competitive area in which market leaders and small technology companies compete. There are Hybrid solutions available from market leaders such as Amazon and Microsoft who provide a combined approach where cloud-based directories link with on-premises IAM systems.

4.3.3. Digital Signatures. Digital signatures are often confused with digital certificates, although they offer entirely different assurances, this form of digital identification is a mathematical technique used to validate the integrity and authenticity of a digital document. It may be viewed as equivalent to a handwritten signature or official seal, whereby offering assurance that digital documents have not been tampered with. It indicates details such as document origin, identity, status and informed consent of the signer. In many countries, including the United States, digital signatures hold the same legal clout as a handwritten signature.

The technique is based on public key cryptography such as RSA that links a private and public key. Solutions for a digital signature create a one-way hash that is subsequently encrypted using the private key. The included data, the encrypted hash and the hashing algorithm create the digital signature. The value of the hash is unique to the hashed data and any change in that data will result in a different hashed value. When the signature is decrypted using the public key and the hashes match, it verifies that the data has not been tampered with. These solutions are also part of a competitive market where market leaders and smaller technology organisations compete.

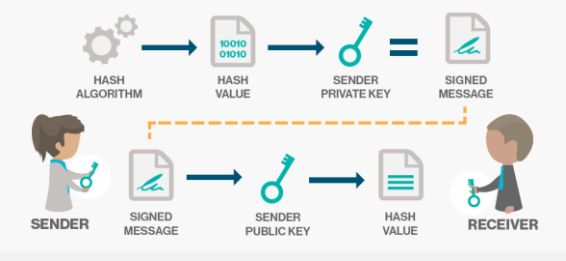

Figure 4. Digital Signatures

4.3.4. Digital Certificates. Digital Certificates are used for secure information transmission over the internet, acting as a type of digital passport for individuals and organisations. The technology relies upon public key infrastructure (PKI) and provides identifying information about the sending party. The security lies in forgery resistance, as the certificates can be verified with their trusted issuing third parties. The certificates contain details including the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate issuing authority to allow the recipient to verify its authenticity. Typically, certificates are proven genuine and valid though a digital signature belonging to a root certificate of a trusted authority. Operating systems and browsers form lists of trusted certificate authorities' root certificates so they may more simply verify subsequent certificates.

The use of these certificates in combination with SSL encryption ensures authentication of the website that users are connecting to; information privacy during the communication cannot be viewed by unauthorised parties and information integrity ensures that the information accessed has not been

altered. This is another area where large and small technology companies compete.

5. Emerging Identification and Authentication Trends

As discussed in previous sections, there has been a major shift from traditional paper documentation (non-electronic) as proof of identity and also an increased need for identity authentication in online transactions. This has increased the need for electronic records required to support e-Government initiatives related to identity and has also improved the popularity of utilisation of off-premises cloud services such as IDaaS. The high prevalence of market leaders offering IDaaS has increased the popularity of this type of IAM and authentication.

5.1. Identity on the Blockchain

Another emergence is the use of blockchain for identity. Many organisations are now offering the utilisation of distributed ledger technology based upon the blockchain data structure as a new approach to identity management [18]. This has given rise to technology that may potentially up-end the current dominant approaches to storing and accessing digital identities in identity management [19]. As a characteristic of distributed ledger technology, this may successfully enhance the security, decentralisation, transparency and user control associated with transactions which include identity information. The landscape of Identity on the blockchain is currently being shaped by three main organisations, uPort [20], ShoCard and Sovrin [18]. This type of technology is intended to operate as an innovative approach to IAM, rather than replacing traditional paper documentation with a truly digital substitute.

5.1.1. uPort. This open source decentralised identity framework aims to provide identity management for decentralised applications on the Ethereum distributed ledger and also for more traditional applications such as online banking and email. Its structure is hinged on Ethereum smart contracts that provide a decentralised record of data movement. Identity is stored within two smart contracts defined as ‘user’ and ‘proxy’ templates. To utilise this application, users create an asymmetric key pair via a mobile application. This transaction is recorded on the Ethereum distributed ledger as a reference to the public key linked to the ‘controller’ template. The ‘proxy’ template contains a reference to the address of the ‘controller’ template. Once this is complete, only the controller template can invoke the functions of the proxy. The address of the proxy stores a unique uPort identifier. uPort securely maps identity attributes to a particular uPort identifier that is part of a registry of uPort identities. Any entity can query the register, but only the owner may modify the associated attributes. Files on the register are retrieved via their cryptographic hash.

5.1.2. Sovrin. This open source decentralised identity network is hinged upon a permissioned distributed ledger, meaning that although it is public, only permissioned nodes may take part in consensus protocols. These nodes are operated by trusted institutions such as banks, universities and governments. Governance of the operation is overseen by the Sovrin Foundation, a not-for-profit group via a legal agreement called the Sovrin Trust Framework. A user may generate a scaled number of required to contextual separate identities. Each identifier is controlled by a unique asymmetric key pair. The user themselves manages the identifiers via a decentralised identifier specification that stores the identifier itself, a cryptographic public key and associated metadata that allow transactions with that specific identifier to occur. The ledger contains the transactions associated with specific identifiers and is distributed among the permissioned nodes.

5.1.3. Shocard. This application uses distributed ledger technology to fuse a personal identifier with a traditional paper document such as a passport or driver licence and additional identity attributes within a cryptographic hash stored within Bitcoin transactions. This form of identity on the blockchain is used for manual verification of identity as well as online transactions. The Bitcoin element is used for timestamping of the signed cryptographic hashes that store the user’personal identifiers. The scheme incorporates a central server that acts as an exchange service for the encrypted identity data between a user and the reliant party. The mobile application creates an asymmetric key pair for each user and uses the camera to scan the traditional paper document. The scan and the associated data are then encrypted and stored on the device. The signed hash is then embedded into a Bitcoin transaction so that the date may be validated. The generated Bitcoin transaction number is utilised as the user’s ShoCardID and is stored in the mobile device as a pointer to the ShoCard verified seal.

5.2. Online Identity Verification and Trust

There has been a demonstrated requirement for individuals interacting in an online environment to not only prove their identity, but also prove their ‘trustworthiness’. This has encouraged a trend toward solutions that are capable of analysing attributes from a subject’s online interaction and produce a score indicating how trustworthy they are. As an example, *Trooly*, assesses the trustworthiness

and measure of 'real' information contained within a digital footprint. This company was acquired by AirBnB to assess the trustworthiness of individuals offering their properties for letting via an online service. However, this service does not provide a digital identification document.

Another alternative is a service called Hooyu that confirms identity in real time. When a user receives a request to prove identity via email or SMS, Hooyu sends the requesting party a confirmation report that confirms that the details they provided are correct. This is achieved by the user supplying Hooyu with a selfie image, an image of a traditional paper document and also their online credentials. The primary use for this service is personal financial transactions with individuals offering services online such as private temporary property rentals and the purchase of used goods.

6. Conclusion

This paper has offered a review of the history of identity, identification and authentication with a particular focus on modern implementations, current trends and emerging technology. As demonstrated, the requirement for proving one's identity has been present for many thousands of years and the methods by which this is achieved pays homage to the resources and technology that are available at the time. It has also been demonstrated that although 'identity' is an ambiguous and amorphous term that refers to something intangible, through documentation of unique personal identifiers, it is something that becomes quite tangible.

The research conducted has followed the development of identity, including the attributes and traits that are considered to contribute to it. These include standard personal identifiers such as name and date of birth, biometrics such as fingerprints and also social behavioural data such as relationships. The constructs of real and fake identities has been examined, indicating the risks associated with fake identities and how they are obtained and also pinpointed through identity resolution.

Increases in population and transient migration have necessitated a shift toward electronic and digitalised records that accompany electronic documentation such as e-IDs, e-Passports and e-Borders. This major move toward global digitalisation has come to exploit the use of the aforementioned personal identifiers and new biometric technologies. These technologies may still be considered two-factor authentication as they include a document containing a smart chip and an electronic record that is linked to a username and password.

Increased utilisation of online services has also necessitated a requirement for individuals to prove their real-world and digital identities through technologies such as IAM, IDaaS, digital signatures and digital certificates offering innovative approaches through ever growing and improving cloud service solutions.

Finally, emerging identity trends have shown an interest in providing measures of trust in a user. Further future-proofing technologies aim to utilise novel and innovative blockchain technologies to store identities, however these are for the purpose of IAMs and online transactions, not as a replacement for traditional paper documentation.

The clear message demonstrated through this research is that the trend is certainly leaning toward 'tangible' identification being phased out and replaced by a substitute 'intangible' digital representative. However, a true 'digital identification' alternative that proves a real-world identity without traditional paper documentation has not evolved as yet.

References

[1] J. Blue, J. Condell, (2017), 'Identity Document Authentication using Steganographic Techniques: The Challenges of Noise', Ulster University, 28th Irish Systems and Signals Conference, Killarney, Ireland.

[2] J. Blue, J. Condell, (2018), 'Identity Document Authentication using Steganographic Techniques: The Challenges of Noise', Ulster University, 28th Irish Systems and Signals Conference, Killarney, Ireland.

[3] M. Cavna, (2013), '"NOBODY KNOWS YOU'RE A DOG': As iconic Internet cartoon turns 20, creator Peter Steiner knows the joke rings as relevant as ever', The Washington Post, (online) https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600 -f98d-11e2-8e84-c56731a202fb_blog.html?noredirect=on&utm_term=.1838265bcd92.

[4] National Institute for Standards and Technology, (2017), 'Digital Identity Guidelines', NIST Special Publication 800-63-3, June, 2017.

[5] G.A. Wang, H.C. Chen, J..J. Xu and H. Atabakhsh, (2006), 'Automatically detecting criminal identity deception: an adaptive detection algorithm', IEEE Transport Systems Management, Part A-Systems Humans 36, pp. 988–999.

[6] United Kingdom Home Office, (2002), 'Identity Fraud: A Study', (online) http:// www.homeoffice.gov.uk/cpd/id_fraud-report.pdf.

[7] H. Köpcke and E. Rahm, (2010), 'Frameworks for entity matching: a comparison'. Data and Knowledge Engineering, Elsevier, Volume 69, Issue 2, page 197–210.

[8] International organization for Standardization, (2011), 'Information technology -- Security techniques -- A

framework for identity management -- Part 1: Terminology and concepts', ISO/IEC 24760-1.

[9] European Parliament, (2018), 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC'.

[10] E.A. Whitley and I.R. Hosein, (2008), 'Doing the politics of technological decision making: due process and the debate about identity cards in the U.K.', European Journal of Information Systems, Volume 17, Issue 6, pp. 668–677.

[11] P. Seltsikas and R.M. O'Keefe, (2010), 'Expectations and outcomes in electronic identity management: the role of trust and public value' European Journal of Information Systems, Volume 19, Issue 1, pp. 93–103.

[12] D. Lyon, (2009), 'Identifying citizens: ID cards as surveillance' Polity Press, Cambridge, UK.

[13] E. Wihlborg, (2013), 'Secure electronic identification (eID) in the intersection of politics and technology', International Journal of Electronic Governance, Volume 6, Issue 2, pp. 143–151.

[14] U. Melin, K. Axelsson, and F. Söderström, (2016), 'Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective', Emerald Insight, Transforming Government: People, Process and Policy, Volume 10, Issue 1, pp. 72–98.

[15] J.H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk and R.W. Schreur, (2006), 'Crossing Borders: Security and Privacy Issues of the European e-Passport', IWSEC 2006: Advances in Information and Computer Security, pp. 152-167.

[16] International Civil Aviation Organisation (ICAO), (2015), 'Machine Readable Travel Documents', Document 9303, Seventh Edition.

[17] Identity Management Institute, 2018), 'Identity and access management market analysis', (online) https://www.identitymanagementinstitute.org/identity-and-access-management-market-analysis/.

[18] Andrew Tobin and Drummond Reed, (2017), 'The Inevitable Rise of Self-Sovereign Identity', The Sovrin Foundation, September.

[19] U. Melin, K. Axelsson, and F. Söderström, (2016), 'Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective', Emerald Insight, Transforming Government: People, Process and Policy, Volume 10, Issue 1, pp. 72–98.

[20] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, (2017) 'uPort: A Platform for Self-Sovereign Identity'.

.