The British Blockchain Association

The British Blockchain Association®
Advocating Evidence Based Blockchain

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

18 November 2025

The Rt Hon Sir Keir Starmer KC MP
Prime Minister
10 Downing Street, London, SW1A 2AA
keir.starmer.mp@parliament.uk

Re: **A Blockchain-Based Digital Identity for the United Kingdom**

Dear Sir Keir,

Parliament is scheduled to debate, on 8 December 2025, a petition opposing the introduction of digital ID cards that has amassed widespread public support, and as of today, has garnered almost 3 million signatures [1]. As President of the British Blockchain Association, the UK's leading industry body advancing evidence-based adoption of Blockchain technologies, I am writing to ask whether the Government has considered a decentralised, privacy-preserving Digital Identity framework based on Distributed Ledger Technology and Zero-Knowledge Proofs. Given parliamentary debates on the risks of centralised digital ID systems, widespread public concern, and global best practices, a self-sovereign, citizen-controlled model could offer a secure, ethical, trusted, and future-proof path for the UK.

The UK's Strategic Context

In the recent past, several parliamentary debates have examined the feasibility of a Digital ID for the UK. This includes contributions by Rt. Hon. Viscount Camrose, a member of the APPG on Blockchain Technologies and Shadow Minister for Science, Innovation & Technology, during the 14 October 2025 House of Lords debate, where he opposed a Digital ID on grounds of privacy, civil liberties, inclusion, and high costs, while advocating for a decentralised blockchain design to enhance security and privacy. Camrose remarked: *"Can they [Government] please ensure that the system is designed as a decentralised tool, using the blockchain to give citizens privacy and security*?" [2]. In another debate in the House of Commons on 13 October 2025, Stella Creasy MP remarked on the costs of the proposed Digital ID: "…*the costings that we have seen are about £1 billion to £2 billion to create the system and another £100 million each year to run it.*" [3].

Similarly, the 21 October 2025 Commons debate on Mandatory Digital ID [4] highlighted risks of data breaches, surveillance, digital exclusion (affecting those without access), and doubts over its effectiveness in tackling illegal migration, without a manifesto mandate. Earlier debates on the Data (Use and Access) Bill [HL] in May 2025 emphasized the need for trusted, interoperable digital identities without centralized systems, aligning with calls for offline alternatives and privacy safeguards [5]. On 11 November, the Northern Ireland Assembly debate unanimously opposed mandatory digital ID [6] highlighting surveillance risks and the need for federated, privacy-focused alternatives. In a HOL debate, Lord Clement Jones noted that the platform to be used to build the digital identity, GOV.UK's One Login, has had security failures that have been repeatedly and

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

publicly criticised. He noted that a GovAssure assessment found that One Login was meeting only about 21 of the 39 required outcomes in the NCSC Cyber Assessment Framework [2].

These viewpoints are not necessarily a rejection of digital progress - rather, they should catalyse the development of a privacy-first, citizen-controlled, cryptographically secure, decentralised identity model built on principles that command public trust. A Self-Sovereign Identity (SSI) framework, built on distributed ledger technologies (such as blockchain), Zero-Knowledge Proofs (ZKPs), verifiable credentials (VCs), decentralised identifiers (DIDs), and advanced cryptography would address citizens' concerns regarding surveillance, centralisation, and mass data collection. Unlike a single, centralised repository of citizen information, SSI vests control of personal data with the individual, enables secure verification without data over-collection, and aligns fully with UK values of liberty, privacy, and proportionality. These systems could help mitigate risks and drive efficiency, inclusion, and trust, imperative for a modern Britain.

The Risks of Centralised Digital Identity

A traditional centralised digital ID model would expose citizens to several vulnerabilities, including cyberattacks and data leaks. Centralised systems create a single-point-of-failure "honeypot" for hackers, as demonstrated by major breaches worldwide. For instance, the 2017 Equifax breach compromised the personal data of 147 million people, including names, Social Security numbers, and birthdates, leading to widespread identity theft [7]. Closer to home, the NHS has suffered repeated cyberattacks, such as the 2017 WannaCry ransomware incident that disrupted services across 200,000 systems globally and cost the UK health service an estimated £92 million [8]. More recently, in June 2025, a breach of China's centralized surveillance network exposed 4 billion records, highlighting how aggregated data repositories invite large-scale exploitation [9]. In the Philippines, the 2023 Community-Based Monitoring System (CBMS) breach leaked sensitive citizen data, and a surge in breaches in 2025 exposed over 52 million credentials in Q3 alone, underscoring the ongoing risks of centralised registries [10]. Data leaks in such systems not only erode public trust but also amplify long-term harms. Leaked information can be sold on the dark web, enabling fraud that persists for years. In the US, the 2025 Connex Credit Union breach exposed member names, account numbers, and debit card details, affecting 172,000 individuals and illustrating how centralized identity data becomes a prime target for financial crimes [11]. These risks, such as single-point breaches, insider misuse, large-scale data harvesting, exclusion of vulnerable populations, and AI-enabled deception and fabrication could irreversibly damage public confidence in digital governance. Yet, with innovative approaches like cryptographically secure blockchain systems, we can mitigate these vulnerabilities and build a more resilient future.

AI & Deepfake Threats

Compounding these issues are AI-driven threats, particularly fabrication of identities, and emerging threats from deepfakes, which exploit centralized systems to perpetrate sophisticated identity fraud. Deepfake technology such as AI-generated audio, video, or images that mimic real individuals has surged dramatically. Reports indicate deepfake files increased from 500,000 in 2023 to 8 million in 2025 [12], with fraud attempts rising 3,000% since 2023 [13]. In identity

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

verification contexts, deepfakes now account for 1 in 20 failures globally, as seen in a 2,000% growth in attacks over the past three years [14]. For example, AI-powered scams have enabled synthetic identities such as fake personas built from real leaked data to bypass KYC processes in banking, leading to billions in losses; Microsoft reported thwarting $4 billion in AI-fuelled fraud attempts in 2025 alone [15]. In centralized digital ID systems, where vast troves of biometric and personal data are stored, AI can learn from breaches to create hyper-realistic forgeries, undermining authentication and enabling impersonation at scale. Leaked data further fuels this fabrication, allowing adversaries to generate undetectable synthetic identities that blend stolen information, potentially leading to widespread fraud, electoral interference, or national security threats. In 2025, North America experienced a 1,740% rise in deepfake fraud, with losses exceeding $200 million in Q1 alone [16]. This not only threatens individual privacy but also national security, as adversaries use AI to attack identity controls.

Modernising Digital Identity Solutions: A Global Perspective

Several jurisdictions around the world have started to modernise their Digital ID systems, utilising a combination of different approaches, including distributed ledgers, Zero-Knowledge Proofs (ZKPs), decentralised identifiers (DIDs), Verifiable Credentials (VCs), OpenID Connect (OIDC), and W3C open standards:

1. **European Blockchain Services Infrastructure** (EBSI): The EU's official blockchain-based pan-European network of nodes for verifiable credentials and cross-border digital wallets. Building a similar infrastructure in the UK would provide a credible blueprint for UK–EU interoperability in areas such as qualifications and credentials, trade finance, visas, immigration and digital borders, and public services, to name a few [17].
2. **UAE PASS:** In collaboration with Digital Dubai and Department of Government Enablement, UAE has built a secure national digital identity pass for citizens, residents and visitors in UAE, incorporating blockchain-backed verification features. The UAE Pass includes a digital vault powered by blockchain technology, for storing users' digital documents and sharing them with government departments [18].
3. **Estonia**'s e-ID: Estonia implemented initiatives such as 'keyless signature infrastructure' – KSI, Public Key Infrastructure (PKI) to modernise citizens' access to public services. KSI also carry eIDAS accreditation, the EU trust mark for qualified trust services with legal power for electronic transactions in the European Single Market. [19].
4. **United Nations Blockchain-based Digital Identity**: In a recent case study published in *The Journal of The British Blockchain Association (The JBBA*), UN Joint Staff Pension Fund (UNJSPF) has implemented a blockchain-based Digital Identity system, supporting over 70,000 retirees in more than 190 countries, reducing fraud risk and streamlining "proof-of-life" requirements. Building a similar infrastructure would modernise UK's Department for Work & Pensions (DWP) [20].
5. **Canada** – British Columbia piloted a Blockchain-Based Digital ID (BC Wallet) enable citizens to use a secure digital wallet app for storing and presenting permits, certifications, and licenses, reducing bureaucracy and improving trust without centralising citizen data [21].

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

6. **Brazil** – **Rede Blockchain Brasil**: piloted a blockchain network designed to improve transparency, data integrity and public-sector interoperability [22].
7. **Singapore's ETH Sign** – Integrated with Singapore's Digital ID SingPass, users are able to execute legally binding contracts on the Blockchain, highlighting how decentralised credentials can coexist with national ID systems [23].
8. **Switzerland** – Federal E-ID (expected 2026 Launch): The Swiss Federal Council has selected DID:webvh as the method for Decentralized Identifiers (DIDs), enabling citizens to maintain control over their digital identifiers without relying on a centralized authority. [24].
9. **Malaysia** – MyDigital ID Superapp: A blockchain-powered national digital identity ecosystem that integrates secure verification for government and commercial services, providing a seamless, scalable solution with a focus on privacy and user-controlled credentials [25].
10. **South Korea** is testing a Blockchain-based Mobile ID Card which allows citizens to use it for banking and other services. The digital ID holds the same legal weight as the physical card but uses blockchain, encryption, and biometrics for enhanced security, and a user can only link it to one smartphone. Issuance involves verifying one's identity at a community centre and using either an IC-chip embedded physical card or a QR code [26].
11. **Bhutan's National Digital Identity on Blockchain:** Bhutan has officially built its National Digital Identity (NDI) platform on Blockchain to boost security and resilience. The move positions Bhutan as the first nation to anchor a sovereign digital ID system on Ethereum's public blockchain. The Ethereum Foundation will collaborate with Bhutanese developers to build local blockchain capacity and new decentralized applications. The National Digital Identity (NDI) system uses blockchain for self-sovereign identity, allowing citizens to control and present digital credentials securely [27].
12. **India's Aadhar 2.0:** India's digital identity, built by the Unique Identification Authority of India (UIDAI), has unveiled Aadhaar Vision 2032, with plans to rebuild the entire Aadhaar infrastructure with blockchain integration and quantum-grade security [28].

In addition to the aforementioned examples, there is a growing literature of evidence around blockchain and ZKPs to build decentralised ID systems: **World Economic Forum** [29, 30]; **IBM** [31]; **Consensys** [32]; **NEC** [33]; **Chainlink** [34]; **Ethereum Community** [35]; **a16z** [36]; **Imperial College London** [37]; **IEEE** [38]; Articles and Case Studies [39, 40, 41, 42, 43], and this paper from **Ross Maude,** Chief Digital and Information Officer for the Cabinet Office: *'Blockchain for Trust Challenges in Public Services'*, *The Journal of the British Blockchain Association, 2020* [44].

Collectively, these deployments demonstrate that digital identity at national scale supported by verifiable credentials and, where appropriate, blockchain, delivers significant gains in security, privacy, interoperability, and user trust, while mitigating related risks through decentralized control.

A self-sovereign Blockchain/ DLT based digital identity

Blockchain-based digital identity, often referred to as self-sovereign identity (SSI), allows users to control and manage their personal data with greater security and privacy. Instead of relying on centralized authorities, it uses a decentralized ledger to store verifiable credentials, which users

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

can selectively share with third parties for verification without revealing unnecessary information. This system increases user control and can mitigate the risk of data breaches and identity theft.

SSI empowers those who have rights in relation to their identity ("identity rights holders") to control use of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals and organisations. This design system should empower identity rights holders to protect the privacy of their digital identity data, and to share the minimum digital identity data required for any particular interaction. An SSI ecosystem shall empower identity rights holders and all other stakeholders to easily access and verify information necessary to understand the incentives, rules, policies, and algorithms under which agents and other components of SSI ecosystems operate.

How it works

- Decentralised control: Users store their identity information in a digital wallet, rather than on a central server.
- Verifiable credentials: The issuer (government) creates tamper-resistant digital credentials that are verified and signed on the blockchain.
- Selective sharing: A user can choose to share specific credentials with a service provider by using a QR code or a link
- Instant verification: The service provider can verify the credential's authenticity directly from the blockchain, without needing to contact the original issuer or store the user's data.
- Enhanced privacy: Technologies like zero-knowledge proofs can allow for verification of certain attributes without revealing the full details, such as proving you are over 18 without sharing your birthdate. Users can share only the specific data needed for an interaction, without sharing all their personal information.
- Increased user control: Individuals are in full control of their digital identity and decide who they share information with.
- Improved security: Decentralisation makes it more difficult for hackers to compromise an entire system, and cryptographic methods ensure data integrity.
- Reduced identity theft and fraud: By providing a secure and verifiable way to confirm identity, the risk of fraud is mitigated.
- Streamlined processes: Verification can be instant and automated, simplifying many online and offline processes.

How self-sovereign digital identity and Zero-Knowledge Proofs (ZKPs) technology would function in a UK context

Under an SSI model, citizens use a secure digital wallet to store verifiable credentials issued by authoritative UK institutions. Examples include Home Office (passport, immigration status, Right-to-Work); NHS (NHS number, prescription eligibility); DVLA (driving licence); HMRC (tax); residency (NI contributions); Universities/Employers (qualifications, professional status); DWP (benefits eligibility, pension details); Education Providers (degrees, skills certifications), to name a few. This reduces redundant identity checks, enhances security, gives users more control over

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

their identity and avoids the creation of a centralised "honeypot" database - a vulnerability repeatedly exposed in major breaches.

Zero-Knowledge Proofs (ZKPs) enable verification of a claim without revealing the underlying personal data. Their integration into a UK SSI system would allow:

1. Age Verification: For online gaming, age-gated retail, or alcohol sales—proof of "over 18/25" without revealing name or address.
2. NHS Access: Confirm NHS entitlement without exposing medical history, GP details, or location.
3. Immigration / Home Office Processes: Verify "Settled Status" or Right-to-Work without sharing full passport or visa scans.
4. Financial Services (FCA KYC/AML): Verify identity attributes without transmitting full documents, cutting fraud and reducing onboarding friction.
5. Transport & Security (DfT, Border Force): Digitally verified travel credentials, reducing bottlenecks in airports and major stations.
6. Digital Voting Pilots: Confirm voting eligibility without revealing address, electoral roll details, or political preference.
7. Social Welfare (DWP): Prove eligibility for Universal Credit or pensions without sharing full financial histories, fostering inclusion for vulnerable groups.
8. Education and Skills: Verify qualifications for job applications or further study without disclosing sensitive details, supporting social mobility.
9. Environmental and Civic Participation: Confirm residency for green incentives or community polls (e.g., "eligible for EV subsidy") without exposing addresses, promoting sustainable and democratic engagement.
10. Cross-Border Travel and Trade: Enable seamless EU-UK credential recognition (e.g., "qualified in field" for professionals) via interoperability with systems like EBSI, boosting post-Brexit economic opportunities.

Critically, verification becomes selective and minimal, e.g.:

- Proving age → "I am over 18" (without sharing birthdate)
- Proving residency → "I reside in the UK" (without disclosing address)
- Right-to-Work → cryptographically verified credential (no document uploads)
- Benefits Access → "Income below threshold" (without revealing full financial history)
- Qualifications → "Degree achieved" (without grades or personal details) ZKPs align directly with GDPR's data-minimisation principles and represent a privacy-preserving verification mechanism, offering robust defences against AI manipulation.

The role of Distributed Ledger Technologies in building Digital Identity Systems

Distributed Ledger Technologies such as Blockchains would strengthen national identity by providing features that centralised architectures cannot match, particularly through its cryptographically secure foundation that ensures data integrity and resilience against leaks, hacks, and fabrication:

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

1. **No Single Centralised Database**: Eliminates the need for a monolithic citizen registry vulnerable to mass breaches. Data remains distributed across user wallets and individual issuing authorities, significantly reducing the impact of any single compromise.
2. **Tamper-Evident Audit Trails**: Any attempted alteration by insiders or attackers becomes detectable through cryptographic hashing, strengthening accountability and transparency while preventing undetected fabrication.
3. **Cross-Department Interoperability**: Verifiable credentials allow frictionless interaction between HMRC, NHS, Home Office, DVLA, and private-sector services without re-collecting the same data repeatedly.
4. **Privacy-by-Design**: Verification does not require government or intermediaries to store or re-collect sensitive personal information, with end-to-end encryption safeguarding against leaks.
5. **Reduced Fraud and Administrative Burden**: Digital credentials significantly reduce identity fraud, improve verification accuracy, and cut processing times; mirroring efficiencies seen in digital-first jurisdictions. Blockchain's tamper-proof, time stamped ledger, combined with advanced cryptography like public-key infrastructure (PKI), provides a resilient barrier against AI-driven threats, ensuring that even if data is targeted, its cryptographic security makes fabrication and exploitation far more difficult.

A Proposal for UK Government:

The BBA recommends the following steps:

1. Establish a UK Self-Sovereign Identity cross-departmental Working Group: A cross-government taskforce including Cabinet Office, DSIT, Home Office, NHS, HMRC, FCA, ICO, blockchain industry experts and associations, and digital identity providers.

2. Examine the feasibility of integration of Blockchain and Zero-Knowledge Proofs to proposed Digital ID infrastructures, such as GOV.UK's One Login. Commission an options paper on SSI/ DLT-based digital identity and launch a Blockchain SSI Pilot Programme to explore areas such as Right-to-Work verifiable credentials, DBS and degree credential verification, et al.

3. Adopt "Non-Centralised and Privacy by Default" Principles: Avoid building a single citizen database for identity; instead use decentralised, privacy-preserving, user-held verifiable credentials as the foundation.

4. Publish a UK Digital Identity Roadmap: A transparent, quadruple-helix, user-centric, evidence-based national strategy with parliamentary oversight, including safety and interoperability standards, and privacy safeguards.

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

Challenges and Opportunities

To build an effective national blockchain-based identity, systems must be interoperable across borders, sectors, and platforms. Organisations such as the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C) have worked on common standards like DIDs (Decentralised Identifiers) and VCs (Verifiable Credentials) to support this goal. Open-source projects help build the infrastructure required for global adoption. However, technical standards are only part of the equation – policy frameworks, legal clarity, and cross-sector collaboration are equally vital. That's why conversations and coordination between governments, technologists, and the private sector are so crucial.

While Blockchain and Distributed Ledgers are not a panacea for all challenges posed by a centralised digital ID system, they have shown us that a more transparent, privacy-focused, resilient and efficient system can be built by utilising these technologies. Public trust in digital identity will depend not on the mere availability of a digital ID, but on its architecture. A self-sovereign, privacy-first identity system built on verifiable credentials, blockchain integrity, and zero-knowledge proofs offers the UK a credible, ethical, and future-proof path that directly counters the perils of centralisation, addressing parliamentary concerns on privacy, exclusion, and security. By embracing cryptographically secure distributed ledger solutions, we can turn these challenges into opportunities for innovation, empowering citizens and strengthening our digital economy.

I hope this analysis and these proposals are of value to you and your officials, as you consider the future of digital identity in the United Kingdom.

Yours sincerely,

Professor Dr Naseem Naqvi MBE
President
The British Blockchain Association (The BBA)
https://britishblockchainassociation.org

(I would like to thank the BBA members, editors of the Journal of the British Blockchain Association, members of the APPG on Blockchain Technologies, and advisors at the BBA's Centre for Evidence Based Blockchain for their input in drafting this letter).

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

REFERENCES:

UK Petition and Parliamentary Debates

[1] Parliament will debate the Digital ID Petition on 8 December 2025: https://petition.parliament.uk/petitions/730194

[2] UK Parliament – Hansard, October 2025: Regarding recent parliamentary questions on digital identity and blockchain: https://hansard.parliament.uk/Lords/2025-10-14/debates/693DCE4C-6613-4B8C-9FA0-02566B165F39/DigitalID

[3] UK Parliament - Discussions on privacy and exclusion: https://hansard.parliament.uk/commons/2025-10-13/debates/37D3137B-302E-4E1B-A6E4-0676456F26D0/DigitalID

[4] House of Commons Debate on Mandatory Digital ID (Oct 21, 2025, risks of breaches, surveillance, exclusion): https://hansard.parliament.uk/commons/2025-10-21/debates/7ACB6A4E-1A1C-4B1F-8197-E0A4AFA18C7F/MandatoryDigitalID

[5] House of Lords - Data (Use and Access) Bill [HL] (May 2025, emphasis on trusted interoperable digital IDs without centralization: https://hansard.parliament.uk/lords/2025-05-19/debates/AD1D6032-D2DF-453B-B4A7-87FFE6ED1428/Data%28UseAndAccess%29Bill%28HL%29

[6] Northern Ireland Assembly oppose Digital ID: https://www.theyworkforyou.com/ni/?id=2025-11-11.8.1

Data Breaches and Vulnerabilities

[7] Equifax Breach (2017, 147 million affected, names/SSNs/birthdates): https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

[8] WannaCry Ransomware (2017, disrupted NHS, £92 million cost): https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

[9] China Surveillance Network Breach (June 2025, 4 billion records exposed): https://www.csoonline.com/article/4003037/colossal-breach-exposes-4b-chinese-user-records-in-surveillance-grade-database.html

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

[10] Philippines Community-Based Monitoring System (CBMS) Breach (2023, sensitive citizen data leaked):
https://philsys.gov.ph/official-statement-3/
https://manilastandard.net/business/314663590/philippines-data-breaches-surged-49-in-third-quarter-of-2025.html

[11] Connex Credit Union Breach (2025, 172,000 affected, names/account numbers/debit details):
https://www.securityweek.com/connex-credit-union-data-breach-impacts-172000-people

AI-Driven Threats and Deepfake Statistics

[12] Deepfake Files Increase (500,000 in 2023 to 8 million in 2025):
https://keepnetlabs.com/blog/deepfake-statistics-and-trends

[13] Deepfake Fraud Attempts Rise (3,000% since 2023):
https://keepnetlabs.com/blog/deepfake-statistics-and-trends

[14] Deepfake Verification Failures (1 in 20 globally, 2,000% growth in attacks):
https://www.entrust.com/company/newsroom/deepfake-attacks-strike-every-five-minutes-amid-244-surge-in-digital-document-forgeries

[15] Microsoft Thwarted $4 Billion in AI-Fuelled Fraud (2025):
https://www.microsoft.com/en-us/security/blog/2025/04/16/cyber-signals-issue-9-ai-powered-deception-emerging-fraud-threats-and-countermeasures/

[16] North America Deepfake Fraud:
https://variety.com/2025/digital/news/deepfake-fraud-caused-200-million-losses-1236372068/

Global Blockchain/DLT/ Decentralised Digital ID Use Cases

[17] European Blockchain Services Infrastructure (EBSI): EU's blockchain for verifiable credentials and cross-border wallets:
https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/447687044/Home

[18] UAE PASS Blockchain-Based ID: Secure national digital identity for services:
https://uaepass.ae/
https://oecd-opsi.org/innovations/digital-vault/#:~:text=The%20UAE%20Pass%20includes%20a%20'digital%20vault'%2C,documents%20and%20sharing%20them%20with%20government%20departments

[19] Estonia's National Digital Identity + KSI:
https://e-estonia.com/solutions/cyber-security/ksi-blockchain/

[20] United Nations Blockchain-Based Digital Identity (UNJSPF Case Study):
https://jbba.scholasticahq.com/article/142770-unjspf-blockchain-based-digital-identity-solution-for-proof-of-life

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

[21] Canada – British Columbia Blockchain-Based Digital ID (BC Wallet): Verifiable credentials for permits/licenses:
https://www.lfdecentralizedtrust.org/blog/bc-digital-trust-leveraging-hyperledger-tools-for-digital-trust

[22] Brazil – Rede Blockchain Brasil: National network for transparency and interoperability:
https://www.gov.br/ibict/pt-br/central-de-conteudos/noticias/2025/agosto/ibict-passa-a-integrar-a-rede-blockchain-brasil-e-conecta-nos-a-infraestrutura-nacional

https://www.lfdecentralizedtrust.org/case-studies/establishing-a-new-foundation-for-trust-how-besu-helps-governments-meet-citizen-needs-while-rebuilding-credibility

[23] Singapore – Verifiable Credentials Integrated with SingPass:
https://singvc.sg/ ETH Sign and Singapore's SingPass:
https://medium.com/ethsign/an-industry-first-ethsign-integrates-with-singapore-digital-id-singpass-377f34535ffa

[24] Switzerland – Federal E-ID (2026 Launch): Page 3; Decentralized wallet-based framework.
https://www.eid.admin.ch/en/technology

[25] Malaysia – MyDigital ID Superapp: Blockchain-powered for government/commercial services:
https://www.biometricupdate.com/202501/malaysia-to-launch-national-digital-id-super-app

[26] South Korea's Blockchain-Based Mobile ID Card (2025): Digital resident card with legal weight:
https://coingeek.com/south-korea-issues-digital-ids-secured-by-blockchain/

[27] Bhutan's National Digital Identity on Blockchain: Anchored on Ethereum:
https://www.buddhistdoor.net/news/bhutan-integrates-national-identity-platform-with-ethereum-blockchain/

[28] Aadhaar 2.0: India's digital ID goes on the Blockchain:
https://www.livemint.com/gadgets-and-appliances/aadhaar-2-0-india-s-digital-id-goes-quantum-with-ai-blockchain-and-next-gen-security-11762248338574.html

[29] https://widgets.weforum.org/blockchain-toolkit/digital-identity/index.html
[30] https://www.weforum.org/stories/2023/03/digital-id-privacy/

[31] https://www.ibm.com/solutions/blockchain-identity

[32] https://consensys.io/blockchain-use-cases/digital-identity

[33] https://www.nec.com/en/global/solutions/blockchain/blockchain-for-digital-identity.html

[34] https://chain.link/education-hub/blockchain-identity

[35] https://ethereum.org/decentralized-identity/

[36] https://cryptorank.io/news/feed/f4832-a16z-urges-treasury-to-embrace-privacy

The BBA CLG Ltd, Kemp House
124 City Road
London, EC1V 2NX, UK

[37] https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/distinguished-projects/2122-pg-projects/Digital-IDs.pdf

[38] https://ieeexplore.ieee.org/document/10467241

[39] https://pixelplex.io/blog/blockchain-digital-identity/

[40] https://www.sciencedirect.com/science/article/pii/S2096720921000099

[41] https://thedatascientist.com/how-to-develop-a-blockchain-based-digital-identity-system/

[42] https://www.dock.io/post/decentralized-identity

[43] https://www.humanity.org/

[44] Blockchain - A Panacea For Trust Challenges In Public Services? A Socio-technical Perspective – Ali Shahaab, Ross Maude et.al: The JBBA (2020): https://doi.org/10.31585/jbba-3-2-(6)2020

About the British Blockchain Association:

Established in 2017, The British Blockchain Association (The BBA) is the world's leading industry body advancing evidence-based adoption of Blockchain, Cryptoassets, and Distributed Ledger Technologies (DLT). The BBA has advisors, ambassadors, members, partners, and editorial board network in 78 countries across six continents. In 2021, BBA authored the UK's National Blockchain Roadmap. BBA is home to the world's first peer-reviewed blockchain research journal The JBBA - Journal of The British Blockchain Association; The world's first Centre for Evidence-Based Blockchain (CEBB); the world's first trans-national collaboration consortium of 53 countries - BAF - The Blockchain Associations Forum, as well as BBA Fellowships (FBBA), Blockchain International Scientific Conferences (ISCs), Scholars in Blockchain International Symposium (SIBIS) and a host of other world-class blockchain initiatives. BBA also has its headquarters in the Metaverse. In 2022, BBA president was awarded the UK's most prestigious National Honour (King's Honour, MBE) for outstanding services to Blockchain and Digital Assets Technologies. The BBA is the Secretariat of the UK's All-Party Parliamentary Group (APPG) on Blockchain Technologies.

END.

***This letter is published on the Blockchain**. To view the Blockchain metadata and timestamp, visit: https://polygonscan.com/tx/0xee8e57fd54630219e0c9e82b247e77ada28ca747633e72f0c87579a8dcc010d4 , then go to > "more details" > view "input data" > "View input as UTF-8"*