accentureconsulting

REFORM

The future of public service identity: blockchain

Maisie Borrows
Eleonora Harwich
Luke Heselwood

November 2017

#reformblockchain

Acknowledgements

Reform would like to thank Accenture for kindly supporting this paper. The authors would like to thank the nine individuals who participated in semi-structured interviews for the paper. The authors are also particularly grateful to James Canham, Managing Director, Accenture Border Services; Victoria Thorpe, Manager, Accenture Technology Consulting; Alexander Hitchcock, Senior Researcher, *Reform* and two individuals who prefer to remain anonymous, for comments on an earlier draft of the paper. Any errors that remain are the authors' and the authors' alone.

Reform

Reform is an independent, non-party think tank whose mission is to set out a better way to deliver public services and economic prosperity. Our aim is to produce research of outstanding quality on the core issues of the economy, health, education, welfare, and criminal justice, and on the right balance between government and the individual. We are determinedly independent and strictly non-party in our approach.

The future of public service identity: blockchain

Maisie Borrows
Eleonora Harwich
Luke Heselwood

November 2017

Definitions

Identity: set of attributes about a person which can relate to their preferences and personality or information that might be more sensitive such as their biometrics, healthcare records or criminal history. These attributes can be collected and used for a particular purpose, such as verifying that a person is who they say they are, and granting access to goods and services based on those attributes. For example, to buy certain goods, such as alcohol, a person needs to prove they are over 18, which is an attribute of their identity.

Public service identity: various pieces of data (i.e. identity attributes) used to verify a person's identity and allow them to interact with and gain access to government services. This data can vary depending on the government service.

Source: *Reform* interviews.

Blockchain: using cryptography to secure exchanges, blockchain provides a decentralised database, or distributed ledger, of transactions that everyone on the network can see. This network is essentially a chain of computers, also known as nodes, that must all approve an exchange before it can be verified and recorded.

Distributed ledger technology: database spread across multiple sites, countries or institutions (i.e. decentralised), and is typically public (see unpermissioned ledger). Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when participants reach a quorum. A distributed ledger requires greater trust in the validators/operators of the ledger.

Permissioned ledgers: these ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors and makes the consensus process much simpler than unpermissioned ledgers. A permissioned ledger is usually faster than an unpermissioned one.

Unpermissioned ledgers (also known as public ledgers): these ledgers have no single owner, like Bitcoin. Anyone can contribute data to the ledger and there is censorship resistance, which means that no single actor or a minority of actors can prevent a transaction from being added. Participants maintain the integrity of the ledger by reaching a consensus about its state.

Sources: Rosamond Hutt, 'All you need to know about blockchain, explained simply', *World Economic Forum,* 17 June 2016. Zach Church, 'Blockchain, Explained', *MIT Management Sloan School*, 25 May 2017.

The Internet has been described as "the decisive technology of the information age"[1] and blockchain is now reinventing it.[2] The realm of applications of this new technology seems to be limitless from payments to safe data sharing of Internet of Things or healthcare data. It has the potential to enable radical public services transformation in a more profound way than previous technologies. An identity management model powered by blockchain could pioneer this change.

Blockchain is a unique technology in that it allows the control of identity data to move from government to the citizen,[3] securely and efficiently. It would enable citizens to view their public service identity via an identity app on their smartphone and share relevant data with government to access public services.

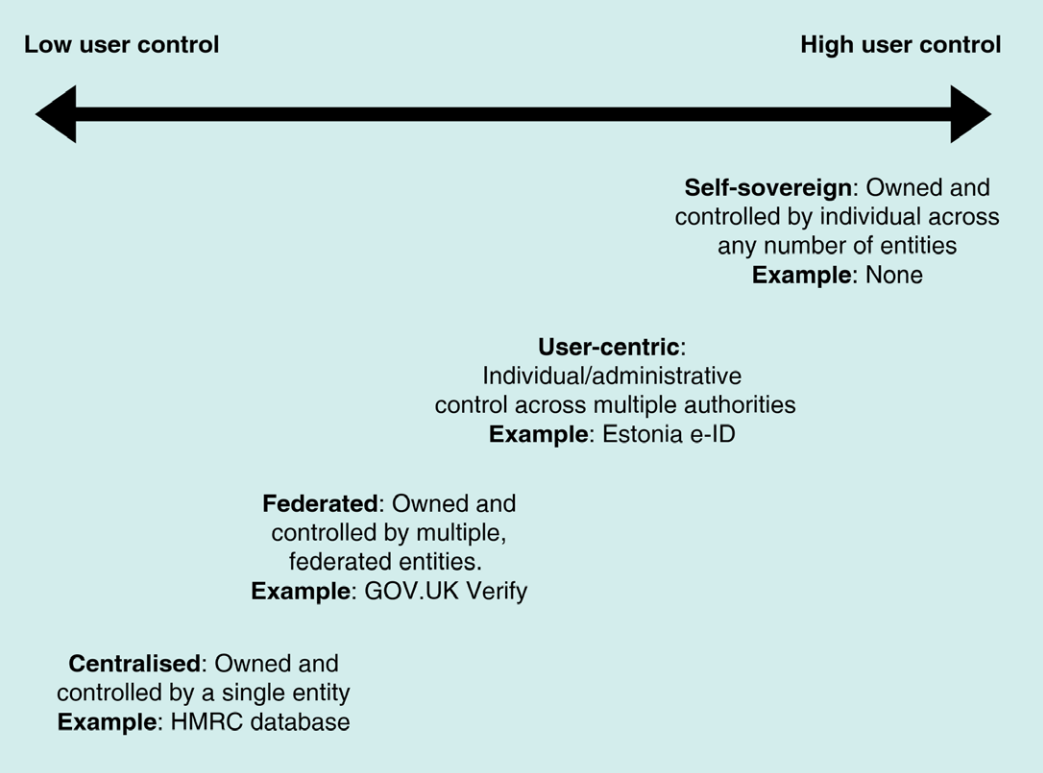
This new model would reimagine the relationship between state and individual, as government would become the verifier, rather than the controller, of people's public service identity. Estonia, Dubai and Australia are trialing the use of blockchain to transform identity management and the UK must do the same if it is to lead the group of digitally enabled nations.

1 Manuel Castells, 'The Impact of the Internet on Society: A Global Perspective', *MIT Technology Review*, 8 September 2014.
2 Brady Dale, 'A Second Internet, Coming Soon, Courtesy of the Blockchain', *The Observer*, 27 September 2016; Jeff John Roberts, 'Blockchain Offers Hope for the Broken Internet', *Fortune*, 27 May 2017.
3 Guy Zyskind, Nathan Oz, and Alex Petland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data* (USA: MIT Press, 2014).

Controlling public service identity

Government should use blockchain technology to make identity management more secure and efficient. This means moving from siloed departments holding different and even contradictory versions of a person's identity to a user-stored identity, in an identity app on a smartphone. User control will move from low to high, with blockchain providing the technology to achieve it (see Figure 1). Unlike today's identity management model, individuals will have access to their public service identity and will authorise who can see it, and in what form.

Figure 1: Framework of digital identity ownership



Source: Adapted from Christopher Allen, *The Path to Self-Sovereign Identity,* 2016.

Today's world: multiple identities

Siloed identities, held by different departments, are insecure, inefficient and inconvenient for citizens.

Centralised data storage is more attractive to hackers.[4] The 2015 cyber-attack on US government databases resulted in the theft of personal information from over 19.7 million people, including social security numbers and fingerprints.[5] Identity theft is at an all-time high in the UK, with almost 173,000 cases in 2016.[6] Paper-based identity verification documents are prone to loss or theft,[7] potentially leading to identity fraud.[8]

Current identity verification processes are also inconvenient for people. Of 25 identity-authentication forms from departments including the Driver and Vehicle Licensing Agency (DVLA), the Home Office, Her Majesty's Revenue and Customs (HMRC) and the

4 See: BBC, 'Turkish Authorities "Probing Huge ID Data Leak"', 6 April 2016; Julie Hirschfeld Davis, 'Hacking of Government Computers Exposed 21.5 Million People', *The New York Times*, 9 July 2015; BBC, 'French Privacy Row over Mass ID Database', 8 November 2016; European Commission, *Horizon 2020 - Work Programme 2016-2017*, 2017, 38.
5 Davis, 'Hacking of Government Computers Exposed 21.5 Million People'.
6 Cifas, *Fraudscape 2017*, 2017.
7 Independent UK Passport Company, 'Lost Passport Guidance', Web Page, 6 June 2017.
8 Information Commissioner's Office, 'Identity Theft', Web Page, 16 May 2017.

Department for Work and Pensions (DWP), 76 per cent requested National Insurance numbers and 68 per cent bank details.[9]

This siloed storage is inefficient for government. Separate databases make it difficult to share information and result in duplication, overlap and contradiction in the information held.[10] As Victoria Thorpe, Manager at Accenture, argues, centralised identity management means "an accurate view of someone's identity is very difficult".

It is little wonder that public trust in data management is low. Several surveys have found this,[11] with one revealing that 13 per cent of people trust government to use their data appropriately, while 46 per cent do not.[12]

Government has attempted to improve identity management through GOV.UK Verify, a scheme where an individual chooses one authorised company to verify their identity to access public services.[13] There are, however, limits to Verify. Control of personal data still sits with government.[14] Uptake of Verify has been slow[15] and departments such as HMRC continue to use their own identity model.[16] This is because Verify provides limited information for certain transactions – meaning that departments need to request and check additional data.[17] The new computer system also has trouble matching information with legacy systems.[18]

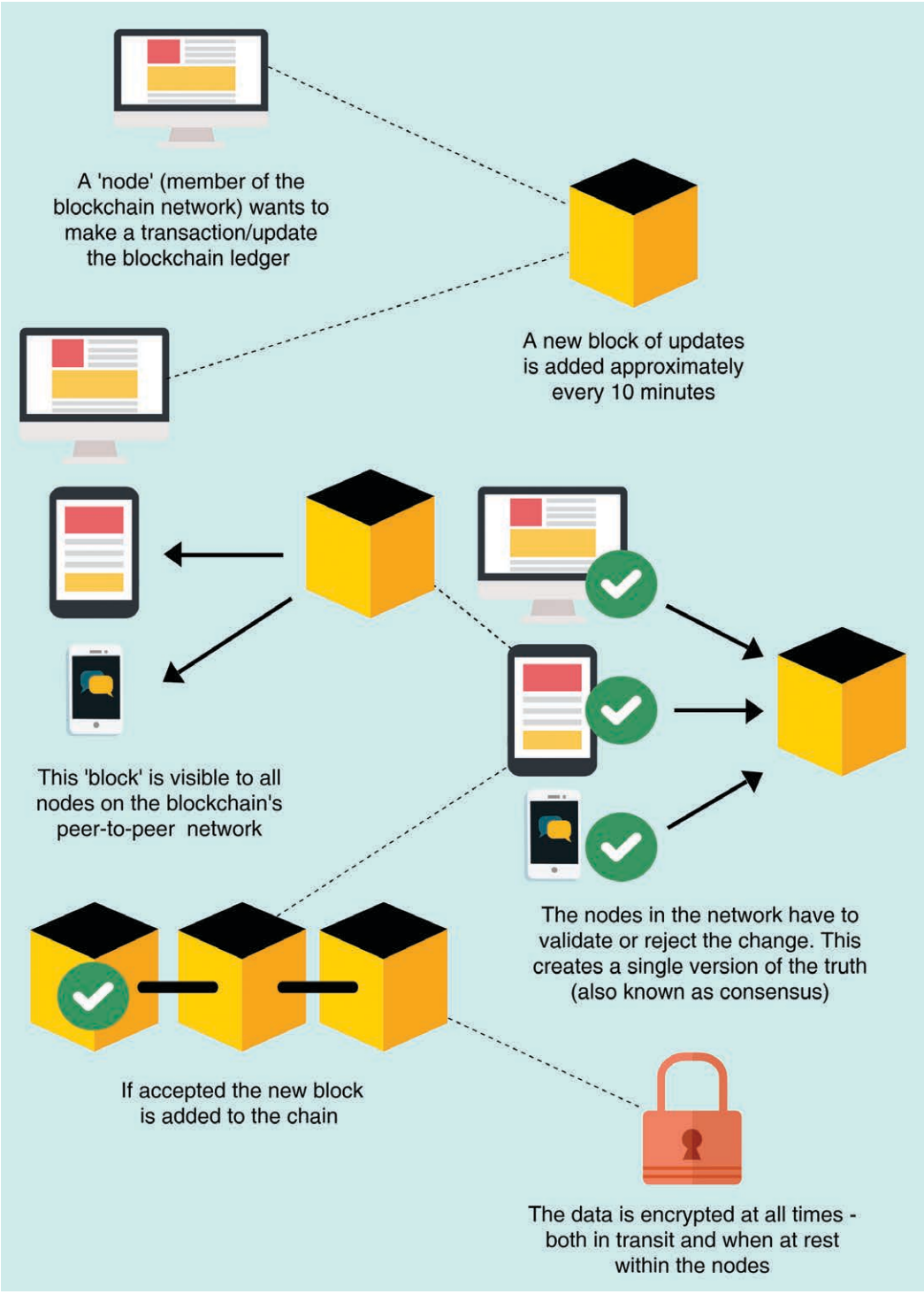
Blockchain: single, secure identity

A new approach is needed – one which is secure, efficient and puts the individual at the centre of identity management. Blockchain offers this.

Blockchain is a distributed, peer-to-peer database that can hold either a record of data sharing or the data itself, on a shared ledger (see Figure 2).[19] The distributed nature of blockchain means control of public service identity can be moved from government to the individual. James Canham, Managing Director at Accenture, describes this as "a shift in data ownership".

9 *Reform* analysis of 25 forms, including passport application, tax credit application, job seekers' allowance and income tax R40 form. These forms are key to accessing services provided by the DVLA, the Home Office, HMRC, and DWP. The data used for this analysis is available upon request.
10 Cabinet Office, *Government Transformation Strategy*, 2017.
11 Royal Statistical Society, *Public Attitudes to the Use and Sharing of Their Data* (Ipsos MORI, 2014); Deloitte and Reform, *Citizens, Government and Business: The State of the State 2017-18*, 2017.
12 Royal Statistical Society, *Public Attitudes to the Use and Sharing of Their Data*, 3.
13 Scott Corfe, *A Verifiable Success* (Social Market Foundation, 2017), 15.
14 National Audit Office, *Digital Transformation in Government*, 2017.
15 Ibid., 42.
16 Kat Hall, 'Don't Tell the Cabinet Office: HMRC Is Building Its Own Online ID System', *The Register*, 24 May 2016; Rebecca Hill, 'HMRC Confirms It Will Use Alternative to Flagship GOV.UK Verify Identify Service', *Civil Service World*, 14 February 2017.
17 National Audit Office, *Digital Transformation in Government*, 43.
18 Ibid., 43.
19 Government Office for Science, *Distributed Ledger Technology: Beyond Block Chain*, 2016, 17–18.

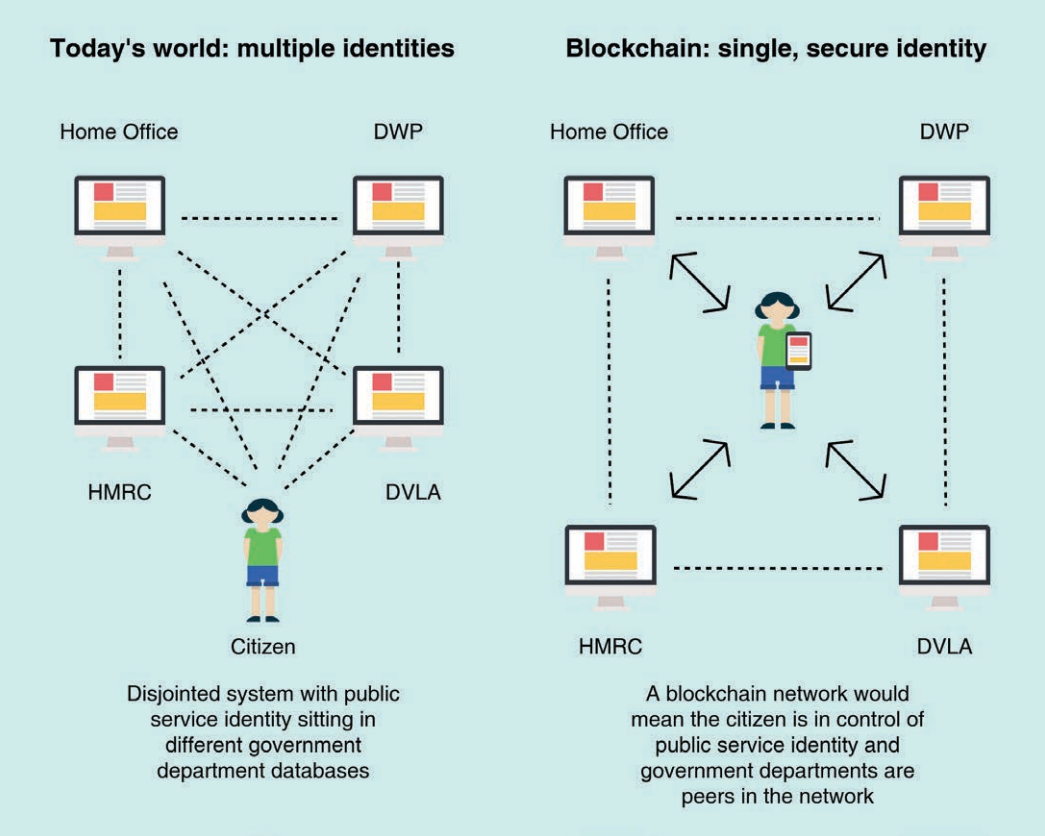
Figure 2: Blockchain



Source: Adapted from *OpenBlockchain*, 2016.

This shift in ownership forms the basis of a new model for identity management (see Figure 3). A blockchain network could be built across several departments and would act as a thin layer on top of current databases. This layer would enable citizens to view their data, via an identity app on their smartphone, and grant government access to it.

Figure 3: A new public service identity model



Source: *Reform* interviews.

An example of how this new public service identity management would work can be found in Estonia, a leader in digital identity management. It has used a blockchain network to make advancements in handing control of data back to the citizen.[20] Citizens have a unique identifier, akin to an NHS number, allowing them to access their health records and review requests by third parties to access their data, meaning that their privacy is ensured.[21]

The new model would be highly secure as blockchain is safer than centralised databases. Information stored on the ledger is encrypted at all times.[22] In addition, its distributed nature makes it very difficult to hack, as it would require simultaneously hacking into a majority of the devices used by the members (i.e. nodes, see Figure 2) on a network.[23] This could reduce the risk of identity fraud.

This model requires a radical shift in the role of government. Government would move from providing data storage to verifying identity. The citizen would no longer simply be a data subject[24] but become the controller[25] of their identity. In practice, an individual would have a set of two encrypted keys, one being completely private and the other public, allowing them to share information with public services.[26] Taking the example of the passport, the individual would only use their public key when verifying their information with the Border Force.

20 Philip Boucher, Susana Nascimento, and Mihalis Kritikos, *How Blockchain Technology Could Change Our Lives* (European Parliament, 2017), 18.
21 Ivan Martinovic, *Blockchains: Design Principles, Applications, and Case Studies* (Working Paper, 2017), 16–19.
22 Sigrid Seibold and George Samman, *Consensus: Immutable Agreement for the Internet of Value* (KPMG, 2017), 12.
23 Zyskind, Oz, and Petland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data*.
24 The Information Commissioner's Office defines data subject as the individual whom particular personal data is about.
25 The Information Commissioner's Office defines data controller as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the way in which any personal data are, or are to be, processed.
26 Tobin Andrew and Reed Drummond, *The Inevitable Rise of Self-Sovereign Identity* (Sovrin, 2016), 11.

Government would retain overall authority over the new identity management model through a so-called permissioned blockchain. It would own the network and would decide who else could access and join it. The decentralised nature of blockchain means that all departments on the network agree to 'one version of the truth' when information is added.[27]

Bitcoin, a popular digital currency, in contrast, uses an unpermissionned blockchain network to document transactions, which means anyone can join and view the information on the network.[28] Given the sensitive nature of public service identity, this type of network would not be appropriate for an identity management model. Highly energy consumptive 'mining' needed in Bitcoin, to secure consensus on the updates made to the network, would not be required. This is because the new model would use a permissioned blockchain, meaning a smaller number of network members would have to reach an agreement on which updates can be added to the blockchain. [29]

The rules of the new identity management model would be codified into smart contracts which are computer codes that can automatically process data and execute protocols on a blockchain.[30] Smart contracts could automatically ensure that government departments are compliant with data protection regulation[31] and that databases are accurately up to date.

Smart contracts also allow the codification of various rights that blockchain network members have, such as what information could be viewed and accessed and in which form. For example, when needing to prove a permanent address in the UK to access a public service, zero-knowledge proof algorithms could allow a citizen to confirm that they have an address without having to give over full address details.[32] Zero-knowledge proof could be a powerful tool to improve public trust in government and make citizens more willing to share data.

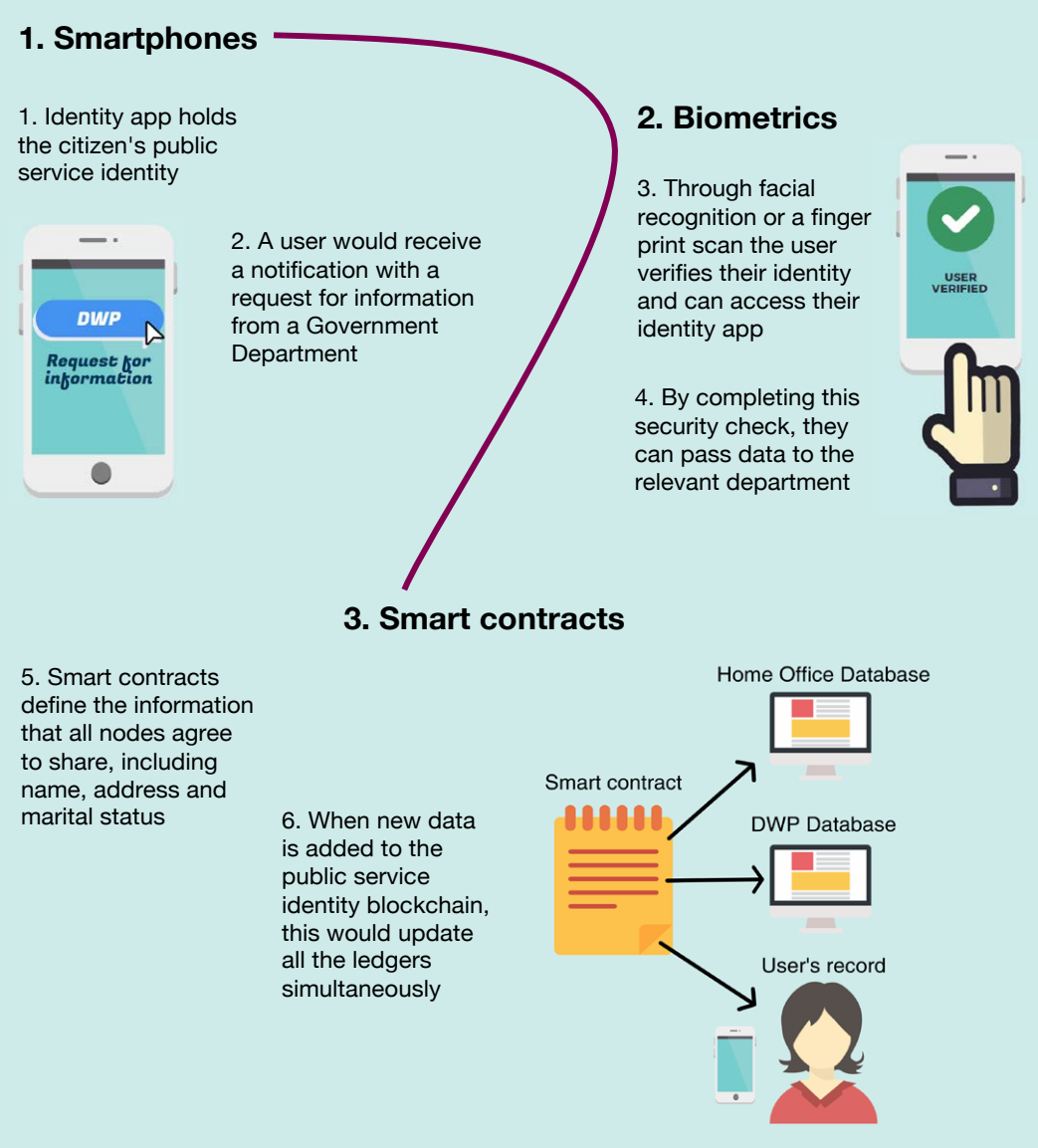
Simon Taylor, Co-Founder and Director at 11:FS, argued that not everyone would want to have the responsibility of controlling their identity data. To gather public support, the practical value of having a single, efficient and secure public service identity must be shown.

Using your public service identity: ID at your fingertips

The blockchain architecture is complex, but its use from a citizen's perspective could not be simpler. When paying tax, claiming benefits or passing through the border, citizens are required to verify personal information with government departments. Through a smartphone, blockchain technology could create a portable and user-friendly digital identity model (see Figure 4).[33]

27 Government Office for Science, 'Block Chain Technology', Video, 2016.
28 Government Office for Science, *Distributed Ledger Technology: Beyond Block Chain*, 2016, 17.
29 Ibid., 17.
30 Ibid., 18.
31 Ibid., 22–24.
32 Ibid., 51.
33 European Parliament, *How Blockchain Technology Could Change Our Lives*, 2017, 19.

Figure 4: A possible use case for a benefit claimant's journey



Source: *Reform* interviews.

Smartphones: sharing data

An identity app – accessible via smartphone – could allow citizens to share data with government departments and access information, such as tax records or benefit claims.

When asked to share personal data with government, citizens would receive a notification on their smartphones, review the request and grant access to that information. For this model to work, smartphones must include security features such as Trusted Platform Module, a microchip that stores cryptographic keys into devices, to address any security concerns.[34]

Estonia's identity system demonstrates the ability of smartphones to hold a citizen's public service identity. Its Mobile-ID system – one of several options available to access their digital identity – uses a special SIM card that stores private keys for authentication, allows citizens to access a host of public services, digitally sign documents and vote through the phone's web browser.[35] The I-Voting system, for example, enables citizens to

34 Government Office for Science, *Distributed Ledger Technology: Beyond Block Chain*, 79.
35 E-Estonia, 'Mobile-ID', Web Page, 2017.

participate in an election from anywhere in the world through smartphones in just three minutes.[36] The Estonia Mobile-ID is not yet powered by blockchain, but demonstrates the capabilities of smartphones for identity management.

Biometrics: securing the system

Access to a public service identity via a smartphone would be underpinned by biometric technology – thus providing two layers of security and improving efficiency.

Angela Sasse, Professor of Human-Centred Technology at UCL, argues that "the second coming of biometrics is upon us". By using facial-recognition technology or fingerprint scans through a smartphone, a citizen could authenticate their identity and interact with public services. An encrypted hash of the biometric data, stored on the smartphone, would be shared through the blockchain, increasing security and giving the individual control.[37]

The Government of Dubai is developing a proof of concept for digital passports that combines biometric verification with blockchain technology.[38] It aims to create a gate-less border, which cuts waiting times and verifies passenger information prior to airport arrival. Before arrival, a passenger would share relevant personal information, via zero-knowledge proof, with border forces and airlines. This would enable passengers to be pre-cleared for travel, reducing the overall waiting time. On arrival, a passenger would simply walk through a biometric 'tunnel' that would scan their face, checking this data against the identity app supplied through the blockchain.[39]

Smart contracts: automatic transactions

The smart contract, which would underpin the new identity management model, would determine what personal information was needed to enable citizens to access public services. When applying for benefits, such as Universal Credit, a claimant would be asked to give consent for their personal information to be shared with DWP as mandated in the smart contract, such as age, income and National Insurance number, through their identity app. Depending on the nature of the specific claim, in some instances where a full disclosure was unnecessary, the smart contract would enable the citizen to provide this information with zero-knowledge proof.

36 E-Estonia, 'I-Voting', Web Page, 2017.
37 International Society of Aeronautical Telecommunications, *Travel Identity of the Future*, 2016, 12.
38 Samburaj Das, 'Dubai Airport to Go Passport-Free with Blockchain Tech', *CryptoCoinsNews*, 12 June 2017.
39 Cara McGoogan, 'The End of Passport Gates? Dubai to Test "Invisible" Airport Checks Using Facial Recognition', *The Telegraph*, 13 June 2017.

Just like the Internet, blockchain will have a profound transformational impact on society. It could radically change the relationship between the individual and the state. For identity management this would mean helping to increase trust in how government uses people's data. Blockchain could deliver more efficient and secure experiences for citizens.

Blockchain technology is still in its infancy but proof-of-concepts have made clear the exciting opportunities it presents for transforming identity management and beyond. Now is the time for the UK government to embrace this technology and remain a truly entrepreneurial, digital state.

BBC. ‘French Privacy Row over Mass ID Database’, 8 November 2016.

———. ‘Turkish Authorities “Probing Huge ID Data Leak”’, 6 April 2016.

Boucher, Philip, Susana Nascimento, and Mihalis Kritikos. *How Blockchain Technology Could Change Our Lives*. European Parliament, 2017.

Cabinet Office. *Government Transformation Strategy*, 2017.

Castells, Manuel. ‘The Impact of the Internet on Society: A Global Perspective’. *MIT Technology Review*, 8 September 2014.

Corfe, Scott. *A Verifiable Success*. Social Market Foundation, 2017.

Dale, Brady. ‘A Second Internet, Coming Soon, Courtesy of the Blockchain’. *The Observer*, 27 September 2016.

Das, Samburaj. ‘Dubai Airport to Go Passport-Free with Blockchain Tech’. *CryptoCoinsNews*, 12 June 2017.

Davis, Julie Hirschfeld. ‘Hacking of Government Computers Exposed 21.5 Million People’. *The New York Times*, 9 July 2015.

Deloitte and Reform. *Citizens, Government and Business: The State of the State 2017-18*, 2017.

E-Estonia. ‘I-Voting’. Web Page, 2017.

———. ‘Mobile-ID’. Web Page, 2017.

European Commission. *Horizon 2020 - Work Programme 2016-2017*, 2017.

Government Office for Science. ‘Block Chain Technology’. Video, 2016.

———. *Distributed Ledger Technology: Beyond Block Chain*, 2016.

Hall, Kat. ‘Don’t Tell the Cabinet Office: HMRC Is Building Its Own Online ID System’. *The Register*, 24 May 2016.

Hill, Rebecca. ‘HMRC Confirms It Will Use Alternative to Flagship GOV.UK Verify Identify Service’. *Civil Service World*, 14 February 2017.

Independent UK Passport Company. ‘Lost Passport Guidance’. Web Page, 6 June 2017.

Information Commissioner’s Office. ‘Identity Theft’. Web Page, 16 May 2017.

International Society of Aeronautical Telecommunications. *Travel Identity of the Future*, 2016.

Martinovic, Ivan. *Blockchains: Design Principles, Applications, and Case Studies*. Working Paper, 2017.

McGoogan, Cara. ‘The End of Passport Gates? Dubai to Test “Invisible” Airport Checks Using Facial Recognition’. *The Telegraph*, 13 June 2017.

National Audit Office. *Digital Transformation in Government*, 2017.

Roberts, Jeff John. ‘Blockchain Offers Hope for the Broken Internet’. *Fortune*, 27 May 2017.

Royal Statistical Society. *Public Attitudes to the Use and Sharing of Their Data*. Ipsos MORI, 2014.

Seibold, Sigrid, and George Samman. *Consensus: Immutable Agreement for the Internet of Value*. KPMG, 2017.

Tobin Andrew, and Reed Drummond. *The Inevitable Rise of Self-Sovereign Identity*. Sovrin, 2016.

Zyskind, Guy, Nathan Oz, and Alex Petland. *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. USA: MIT Press, 2014.

Reform
5-6 St Matthew Street
London
SW1P 2JT

T 020 7799 6699
info@reform.uk
www.reform.uk

ISBN 978-1-910850-15-2