BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES

a thematic report prepared by

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM

EUBlockchain
Observatory and Forum

An initiative of the

European Commission

About this report

The European Union Blockchain Observatory & Forum has set as one of its objectives the analysis of and reporting on a wide range of important blockchain themes, driven by the priorities of the European Commission, and based on input from its Working Groups and other stakeholders. As part of this it will publish a series of thematic reports on selected blockchain-related topics. The objective of these thematic reports is to provide a concise, easily readable overview and exploration of each theme suitable for the general public. The input of a number of different stakeholders and sources is considered for each report. For this paper, these include:

- Members of the Observatory & Forum's Working Groups.
- Government services and digital identity by Dr Allan Third, Dr Kevin Quick, Mrs Michelle Bachler and Prof. John Domingue – an academic research paper prepared by the Knowledge Media Institute of the Open University, one of the Observatory's academic partners.
- Input from participants at the 'Government Services and Digital Identity' workshop held in Brussels on 5 July , 2018.
- Input from the Secretariat of the EU Blockchain Observatory & Forum (which includes members of the DG CONNECT of the European Commission and members of ConsenSys).

CREDITS

This report has been produced by ConsenSys AG on behalf of the European Union Blockchain Observatory & Forum.

Written by: Tom Lyons, Ludovic Courcelas, Ken Timsit
Workshop moderator: Susan Poole
Report design: Benjamin Calméjane
Images: Unsplash

v1.0 - Published on 7 December, 2018

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Contents

Executive summary

European governments have long turned to digital tools to help them both deliver government services and better carry out the business of governing. It's hardly surprising, then, that the blockchain, one of the most significant innovations in data gathering and processing to appear in a long time, would capture the attention of government administrators in the Union.

Much of this interest is based on key inherent properties of the technology. Blockchain, for instance, is very good at **creating trust in information and processes in situations where there are large, heterogeneous sets of stakeholders or users**. Blockchain is also good at creating **trusted audit trails of information** and, depending on how a system is designed, makes it relatively easy to **keep data both private and shareable.** Because blockchains are decentralised, distributed systems with strong automation potential, they can be used to design efficient, inexpensive platforms, potentially leading to **significant cost savings in data processing while increasing the robustness** of the platforms.

These properties could be advantageous in a wide range of use cases. Blockchains can be deployed **to secure and share important data and records**, for example the records of our **identity**, which could be put on chain and used to provide a secure, unique, verifiable identity to all the actors in the digital economy. Blockchains can be used for **asset registries**, for instance with regard to land title, or to improve the securing and sharing of important data like patient health records or educational certifications. With verified data on a blockchain, it could be possible to design trustworthy e-voting systems, too.

Another set of use cases for blockchains revolves around **the monitoring and regulating of markets** of various kinds, supporting governments in their task of protecting consumers and keeping markets safe and viable. Shared ledgers can help governments reduce friction in gathering and aggregating data from participants in the markets they oversee, and may even open a path to **real-time data collection and market supervision**. Shared ledgers could be used to **combat tax fraud and streamline how taxes are calculated and collected**, as well as how governments manage their own expenditures, whether in procurement, entitlements or administration. Blockchains can also help increase efficiency and reduce costs in government operations.

EXECUTIVE SUMMARY

However, there is still a long way to go before we will be able to implement some of these ideas, as there are still technological and regulatory hurdles to overcome. In many use cases it may also be possible to get similar results without using blockchains at all. For this reason, **experimentation needs to continue,** including proofs of concept that weigh **not just the technological feasibility of the solutions but also their economic and social impact.**

To make blockchain's potential a reality, governments will need to lay the right foundations. As we argue in some detail, **digital identity is the fundamental building block** and a key area for governments to focus on. In particular, we feel that governments should support the development of user-controlled, "self-sovereign" identity capabilities. If governments want to successfully deploy blockchain technology for themselves, they will, of course, **need the requisite infrastructure too**, and should explore ways to efficiently make blockchain available to government agencies.

Another important building block, in our opinion, is having **digital versions of national currencies on the blockchain,** for example through blockchain-based central bank digital currencies (CBDCs). Making it possible for legal tender to become an integral part of blockchain transactions will make it easier to reap the benefits of new technologies like smart contracts. On a systemic level, CBDCs could bring the **benefits of decentralisation to inter-bank payments and real-time gross settlement systems**, among other things.

The success of blockchain in Europe will to a large extent depend on government policy. One clear way that governments can drive adoption of the technology is by **using the technology themselves, or by supporting public/private partnerships** (something Europe

EXECUTIVE SUMMARY

has historically done well). **Regulation will play an important role too**. There is no shortage of open issues, from reconciling blockchain's data sharing properties with the data protection provisions of the GDPR to addressing the legal status of smart contracts and digital assets.

How can Europe proceed? In our recommendations section we suggest and expand on the following aspects:

1. Set up the right infrastructure to make sure it is easy and fast for government agencies and institutions to build their own applications in a cost-effective and interoperable manner.

2. The ecosystem would benefit from tailored policies and regulations, clarifying and adapting current frameworks when relevant and implementing new rules if required.

3. Educating the general public, entrepreneurs and civil servants should be a priority.

4. The EU should take the opportunity to drive high-impact projects through Member States and public/private collaboration, as well as dedicated research and development.

Whether or not blockchain technology can fulfil its promise, enjoying widespread adoption by government agencies in Europe, remains to be seen. It seems clear, however, that governments will continue on the path of digitalisation in their quest to offer innovative, efficient and cost-effective e-government services. As we try to illustrate in this report, blockchain technology could be a powerful tool in support of this goal.

Introduction: the government and blockchain

Blockchain technology has been hailed as a revolutionary new means of secure and transparent record keeping and data sharing, with seemingly endless potential uses in a wide variety of sectors. This includes in government settings.

Today, government agencies around the world are looking to blockchain to help make their services more efficient, more cost-effective, more secure and more transparent. Many are also looking at ways in which blockchain might increase trust in government processes, as well as in institutions of governance.

This is certainly the case in the European Union, which has embraced blockchain as an important tool in fostering innovation and supporting the digital single market. To this end, it has, among other things, launched the European Union Blockchain Observatory & Forum, under whose aegis this paper is being written, and plans, through its Horizon 2020 programme, to invest up to €300 million in projects supporting the use of blockchain in a number of sectors. Many Member States have been very active in supporting blockchain ecosystems, starting experiments of their own and announcing actions at the policy level.

Having realised blockchain's potential, European governments are also looking to set an example in its use. In April 2018,[1] 22 member states signed the Declaration for a European Blockchain Partnership (EBP) in order to "cooperate on the development of a European Blockchain Services Infrastructure."[2] With its ambitious goal of identifying initial use cases and developing functional specifications by the end of the year, the EBP should be an important catalyst for the use of blockchain technology by European government agencies.

It will no doubt be a source of important learnings as well. For despite its potential, as a technology blockchain is still in its infancy, nor is it without its risks. Governments have significant responsibilities when it comes to things like data protection, privacy and accountability. Any major change

[1] European countries join Blockchain Partnership, 10 April 2018.

[2] To date, 27 members have signed.

in the way they go about fulfilling these responsibilities has, naturally, to be handled with care.

In this paper we take a look at the potential and pitfalls of blockchain for government services. Our intention is to entice the reader with a look at what is being done today with blockchain in government in Europe and elsewhere, and what, in our opinion, could be done with the technology in the medium term. We also provide our opinion of what Europe needs to do in order to make blockchain a viable option for governments looking to improve how they carry out the work that has been entrusted to them.

The public trust engine: what blockchain can bring to government services

Putting the ebbs and flow of politics and policy-making aside, the business of government administration in a modern, technologically advanced society is an extremely complex undertaking.

Government agencies are responsible for numerous tasks, from implementing policy decisions and delivering a wide range of services and entitlements to regulating markets, collecting taxes and protecting and policing citizens. They also serve a variety of stakeholders, whether it is government to citizen services (G2C), to businesses (G2B), other government agencies (G2G) or their own employees (G2E).

To help, government agencies have long turned to digital tools to support their work. These efforts are often categorised under the heading of **e-government**, defined as the use of digital tools to increase efficiency and reduce the cost of government administration. Digital tools can also help with the business of governing, for example through e-voting, promoting transparency and fighting corruption, and so on. This is generally referred to as **e-governance**.[1]

Europe has traditionally been strong in both areas,[2] but, as the European Commission has previously pointed out in its European eGovernment Action Plan 2016 – 2020, there is much more it could do.[3]

The task should not be underestimated. Planning, building and implementing complex IT systems is difficult in any sector. Government settings, where decisions can be affected by shifting politics and complex procurement rules, can present extra hurdles. Budgets for government projects can also be tight. And, like any large organisation, government agencies are not immune to silo thinking or to administrators resistant to change and new mindsets.

Governments must also adhere to high standards. Ideally, public authorities and agencies administering modern democracies like those in Europe should be both transparent and discrete, fully accountable and fair, efficient and cost-effective, as well as, particularly in the European context, willing and able to work seamlessly across borders.

Governments also do not exist in a vacuum. As society continues to digitise, we will see an exponential rise in the number of participants in the digital economy – not just people and organisations but increasingly machines and autonomous, artificially intelligent agents. This will lead to an explosion in the amount of data that is generated in the world. Government agencies will need to be prepared.

[1] For simplicity's sake, we sometimes use the term "e-government" as a catch-all for both e-government and e-governance, but the distinction is important to keep in mind.

[2] eGovernment - Using technology to improve public services and democratic participation, Davies, R, European Parliament Research Service, September 2015.

[3] See European eGovernment Action Plan 2016-2020.

THE PUBLIC TRUST ENGINE: WHAT BLOCKCHAIN CAN BRING TO GOVERNMENT SERVICES

With this in mind it is hardly surprising that blockchain has captured the attention of government administrators.

Firstly, blockchain technology is very good at creating trust in information and processes in situations where there are large, heterogeneous sets of stakeholders or users. Unlike traditional, centralised databases, where a single entity is generally reponsible for collecting, securing and sharing information, blockchain platforms are based on decentralised, shared databases that are updated and verified by the community of users. With "smart contracts", users can also pre-agree on processes for how to use the data, which can then be automated in the knowledge that they will be carried out as agreed.[4] Considering the resources currently expended in the **checking, double-checking and reconciliation of data collected by public administrations**, there is reason to believe that substantial cost and time savings can be achieved by such decentralised, real-time synchronised databases powered by blockchain technology.

Secondly, blockchain is very good at creating **trusted audit trails of information, making it simple to create platforms to track when and where data was entered, what it has been used for, who has accessed it**, and so on. This can greatly increase **transparency** in terms of data handling and processes and – important in a government setting – make it difficult to misuse or falsify information. Such audit trails can also greatly increase accountability.

Thirdly – and somewhat paradoxically – blockchains also make it relatively easy to keep data both private and easily shareable. Depending on how a system is designed, administrators can develop complex permissioning schemes to control who has access to what kinds of information, what can be shared by whom, and so on. Of course, this can be achieved with regular databases as well. Where blockchains shine is in enabling such capabilities among large, diverse groups without relying on or having to trust a single authority to do the job.

Finally, because blockchains are decentralised, distributed systems with strong automation potential, they can be used to design efficient, inexpensive platforms, potentially leading to significant cost savings in data processing while increasing the robustness of the system.

That said, it is important to keep in mind that blockchain technology is by no means the solution to every problem. There will be many use cases where a centralised database, operated by a single trusted government entity, will do a great job at delivering the promise of digital government services, with no immediate need to employ blockchain technology.

To get a picture of where blockchain could potentially make a difference, we are now going to take a look at some examples.

[4] For an overview of blockchain, please see the Appendix.

Use cases: putting blockchain to work in government services

To illustrate the many ways in which blockchain could be applied in government services we have put together an overview of some of the most promising use cases, as well as some early efforts to address them with blockchain solutions.

SECURING AND SHARING IMPORTANT DATA AND RECORDS

One of the most important set of use cases for blockchain in government is around the verification of records and sharing of data of various kinds. The following are among the most promising of such cases.

1. Identity

As we argue in more detail below, perhaps the most essential and enabling use case for blockchain in government services is in the realm of digital identity.

Governments, after all, are not only the source of key identity information for us as citizens – from the official registration of our birth to the confirmation of our demise through the issuance of our death certificate – they also need to be able to unambiguously identify citizens and stakeholders if they are to provide services to them. What holds for humans is equally true for organisations, whether companies or associations, as well as assets and, increasingly, machines and other autonomous agents.

In an ideal world, every actor in the digital economy would have a unique, verifiable identity that was secure and private yet capable of providing sufficient proof of identity in any online context, without the user having to appeal to a third-party authority and without revealing more information than is necessary for the transaction at hand.

As this has proven difficult to achieve with traditional, centralised technologies, some governments are looking to blockchain to try to realise this ideal.

In Switzerland, the city of Zug made headlines last year by issuing the first publicly verified blockchain-based identity credential to residents,[1] which they have subsequently used for e-voting[2] and renting e-bikes.[3] The Finnish government has worked with a local startup to introduce a blockchain-based identity system for refugees in Finnish camps that is linked to a debit card the refugees can use to purchase food and other necessities.[4] As part of the work of developing a European Blockchain Service Infrastructure, the European Blockchain Partnership is also exploring the use of eIDAS-compliant but more decentralised identity systems on a Europe-wide level.

[1] Zug And uPort See First Citizens' Identity Registered On The Ethereum Blockchain, ETHNews, 17 November, 2017.
[2] Switzerland's first municipal blockchain vote hailed a success, SwissInfo, 2 July 2018.
[3] Zug residents can now ride e-bikes using their uPort-powered Zug Digital IDs, Alice Nawfal, Medium, 14 November, 2018.
[4] How Refugees are Helping to Create Blockchain's New World, Wired, 14 April, 2018.

2. Title/asset registrations

One of the earliest use cases proposed for blockchains was for title or asset registrations. This makes sense, as registering "title" to an asset is a core function of blockchains. Originally, this was for title to a certain amount of a crypto-asset but the idea can easily be extended to almost any asset that can be represented in digital form.

Blockchain has long been proposed for use in land registries, for instance. This was initially the case above all in developing countries looking to fight corruption by local officials who could "steal" land by altering paper-based records. We have seen blockchain projects for example in Africa[5] and India[6] aimed at attacking this problem.

As anyone who has bought and sold a house in Europe knows, even in developed regions transferring title can be a slow, laborious and expensive process. Often paper-based, it involves coordination and verification between many different entities, including government agencies, banks, lawyers and the parties involved.

Blockchain technology offers the possibility to radically streamline such processes. In Sweden, the Lantmäteriet recently carried out its first successful test transaction of a fully blockchain-based transfer of title.[7] In the UK, HM Land Registry is testing blockchain in its bid "to become the world's leading land registry for speed, simplicity and an open approach to data".[8]

The same processes can, of course, be used to secure information about almost any kind of registration, for example businesses or automobiles. Some of these use cases could have significant social impact, such as registering firearms and ammunition to track their use or abuse.

3. Healthcare

Another important use case for blockchain is in publicly provided healthcare. There are two main areas.

First, blockchain can potentially improve the securing and sharing of patient medical records. Today, medical records are typically kept separately in doctors' offices and hospital databases. They are still often shared manually, and not always in a very secure way.[9] This is a problem, considering the sensitive nature of the data. It can also get complicated in a multi-provider system, where various people and institutions have to make inputs to a patient's data.

Blockchains are very good for such scenarios, providing a clear audit trail of inputs by multiple sources, and ensuring that data is not manipulated or corrupted once it is saved. Estonia, which has established a national Electronic Health Record,[10] is contemplating using a blockchain-based registry to ensure the correct handling of sensitive health data by securing the entry of new data into the record and providing an immutable audit trail of how the data has been used. In Sweden, there is an initiative to develop a national blockchain for health records to give citizens more control of their data.[11]

[5] Bitland's African Blockchain Initiative Putting Land On The Ledger, Forbes, 5 April, 2016.

[6] Indian State Partners With Blockchain Startup for Land Registry Pilot, Coindesk, 10 October, 2017.

[7] Sweden's Land Registry Demos Live Transaction on a Blockchain, Coindesk, 15 June, 2018.

[8] HM Land Registry to explore the benefits of blockchain, Gov.uk, 1 October, 2018.

[9] Let's get real about what's up with WhatsApp in the NHS, Felix Jackson, HSJ, 3 July, 2017.

[10] Estonian e-health record.

[11] A Nordic way to blockchain in healthcare, HiMiss Europe, 26 February, 2018.

Health data is not just important for patients. Anonymised, it can be a great source of information for researchers and authorities. In Europe, MyHealthMyData (MHMD), which is being funded under the EU Horizon 2020 programme, aims to use blockchain to create the world's first open biomedical information network. Among other things, it would encourage hospitals to make anonymised data available for open research and make it easier for citizens to take control of their health records.[12]

Let us be clear: in the above use cases, what is proposed is generally not the storage of the data itself in a blockchain network. Rather, the blockchain is used to store proofs that off-chain data is genuine, and/or to store a record of who has access to what data. This allows data owners to store their personal and medical data in secure locations of their choosing, rather than allow large number of health providers to store the same data (sometimes in antiquated and porous IT systems).

4. Educational certification

Educational certification is another area where important personal data tends to be kept in siloed databases, typically the universities or schools that issue the diplomas. Getting access to this information in order to prove credentials can be a laborious undertaking. Degrees can also be relatively easily falsified, posing problems for those who are trying to verify these credentials.

Blockchain-based systems can help here on both sides of the equation. As with health records, they can allow individuals to take control of their educational credentials through the possession of verified records, which they can then use as needed. Because such credentials can be easily verified, employers or others who rely on them can have more trust in their veracity.

The potential of such an approach has been widely recognised[13] and many projects have already started. The University of Nicosia, for instance, already issues academic certificates that can be verified online via a blockchain.[14] In Malta, the government is teaming up with a startup to build a prototype system to do the same.[15] A consortium of Malaysian universities is building a blockchain-based platform to combat fake degrees,[16] while a French startup is looking to use a blockchain network for the issuance and sharing of university and other degrees.[17] The European Blockchain Partnership has selected diploma sharing on a blockchain as one of the promising use cases to be deployed over the European Blockchain Service Infrastructure, a use case that is backed by several Member States.

5. E-Voting

Voting is another important use case dependent on the transmission of private but verifiable data, and e-voting has long been a tantalising prospect for e-government. If citizens could easily and securely vote from any location – for example, using smartphones or personal computers – we could, in theory, develop more participatory democracies, voting more often on more issues.

[12] MyHealthMyData.

[13] Blockchain in Education, EU Science Hub.

[14] Academic Certificates on the Blockchain, University of Nicosia Blockchain Initiative.

[15] Malta Pilots Blockchain-Based Credentials Program, IEEE Spectrum, 5 June, 2018.

[16] University consortium set up to authenticate degrees using blockchain technology, New Straits Times, 9 November, 2018.

[17] bcdiploma.com

Yet e-voting has yet to catch on in a large way. One problem is trust: to many it can seem easier to manipulate digital voting systems than those using paper ballots, which are counted in public with observers on hand. This can make people wary of the technology.[18]

With verified data on a blockchain, it may be possible to design e-voting systems that are much more transparent and trustworthy, while preserving confidentiality. In such systems, election authorities would issue voting credentials to users directly that could be used to cast anonymous ballots. Through various techniques it could then be possible to automatically count those ballots, ensure that no votes were cast more than once and prove the validity of the count without revealing the identity of those who voted.

These are all worthy aims. Yet the devil is in the details. Blockchain-based e-voting means replacing trust in election authorities with trust in the protocol. That means trust that the protocol works as advertised (no bugs or flaws) and that it cannot be manipulated. These are major caveats. E-voting systems will also most likely need to rely on some more fundamental digital identity system, allowing voters to be identified (registered) so as to ensure that only eligible voters participate. People will need assurances that both voter authentication and vote counting are indeed more trustworthy with blockchain e-voting than with current approaches.

This has not stopped people from working on solutions. As mentioned above, the citizens of Zug used their blockchain IDs earlier this year to conduct the city's first blockchain-enabled e-vote. While only consultative in nature, it may be one harbinger of things to come. Similar blockchain-based e-voting projects are underway in areas as far flung as West Virginia[19] and Moscow.[20] E-voting is also mentioned as a possible use case in the European Parliament's Blockchain Resolution of 3 October.[21]

MONITORING AND REGULATING MARKETS

One of the key tasks of government is to regulate and monitor markets to protect consumers, make sure markets remain viable and ensure that laws are adhered to. To do this, regulators need to know what is going on in those markets, which, in turn, means they need data.

This data can be hard to come by. In many cases – the financial services industry is a good but by no means the only example – governments rely on companies themselves to supply the legally required information (self-reporting). In other cases, they carry out inspections or use other means to try to gather the information they need.

Such methods can be problematic. In the case of self-reported data, governments are dependent on the reporting entity for the accuracy of the information. This leaves the door open to fraud. But even honest companies – which represent the vast majority – can make mistakes or not be in a position to supply accurate data. Self-reporting also often entails a significant time lag. In fast-moving industries

[18] Why Online Voting Is a Danger to Democracy, Stanford Engineering, 3 June, 2016.

[19] West Virginia Introduces Blockchain Voting App for Midterm Election, Slate, 25 September, 2018.

[20] Russia Is Leading the Push for Blockchain Democracy, Coindesk, 21 February, 2018.

[21] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)).

and markets, such a lag means information is obsolete by the time it arrives at the regulator. Carrying out inspections and audits, on the other hand, is expensive. As such methods are essentially just "spot checks", they only provide a partial picture of what is going on.

Once gathered, regulators have to aggregate the information they have received. This too presents its challenges, particularly if the data comes from multiple sources in different formats. Because of the time lags involved, regulators can generally only step in after the fact, writing rules to try to prevent the next crisis instead of intervening to prevent the current one from getting out of hand. Reporting also tends to be expensive and time-consuming for companies, which, depending on the industry, often have to make costly investments in compliance teams and infrastructure.

Blockchain technology could conceivably help address such issues. Having a shared ledger can simplify data collection. Instead of self-reporting after the fact, regulators could more easily request real-time reporting from institutions like banks or manufacturers, potentially by "plugging directly into" their systems or by developing a shared, blockchain-based platform for a given industry that unites companies, regulators and other stakeholders.

In manufacturing supply chains, such platforms could make good use of automation through sensors that send data directly to the blockchain. This would allow regulators to replace inspections with direct, real-time monitoring of products during their lifecycle. Such capabilities could be particularly effective in "critical" supply chains, like foods and pharmaceuticals, the protection of which are essential to public safety.

There are many potential advantages to such approaches.

By using shared ledgers to reduce friction in data supply/gathering, governments can in theory greatly increase the amount of data they receive from regulated entities, as well as receive data from more sources. Blockchain should also make it easier for governments to verify information, increasing their trust in it. Secure, trustworthy audit trails of the kind provided by a blockchain ledger would also be extremely useful when it comes to carrying out investigations or in the case of litigation.

Having a shared ledger implies a shared data format. This should make it easier for regulators to aggregate the information they receive and turn it into meaningful insights. All of this would give regulators a far richer, more accurate and more timely view of the state of markets or supply chains at any given time.

This could contribute to public safety while reducing fraud. With real-time data in financial markets, for instance, governments could spot trouble at a bank or insurance company much more quickly than in the past and potentially take proactive measures to ring-fence it. In critical supply chains, governments would likewise become more quickly aware of problems like bad drugs or tainted food. This would allow them to intervene more quickly and accurately in the event of product recalls or public advisories. Such systems could also be useful in monitoring critical infrastructure like energy or air traffic, allowing for more efficient oversight but also intervention in an emergency. In the same vein, we can imagine that public-health officials could benefit from more real-time data in an epidemic, or disaster-relief officials during a natural disaster. Governments could also better monitor dangerous goods, like chemicals or firearms, by having a much clearer picture of where they are and how they are used.[22] This too could contribute to improved public safety.

To work, such use cases will require that all actors in a market are represented in the platform. This can take different forms. In theory, regulators could mandate a single, market-wide blockchain for a given sector. More likely, however, will be the evolution of a multitude of industry-specific blockchains. These, in turn, will likely be themselves connected (or "interoperable") through various bridges and could provide interfaces to allow governments direct access to the data.

Important use cases from a regulatory perspective include know-your-customer (KYC), anti-money laundering (AML) and countering terrorism financing (CFT) checks. Blockchain-based shared customer and business registries, for instance, could greatly reduce KYC/AML compliance costs by allowing all entities involved to share KYC/AML information in a secure way. This could also be of interest to individuals and businesses, which would profit from a single onboarding experience instead of having to produce their (generally paper-based) credentials for a KYC check every time they sign up at a new financial institution. Last year, Singapore carried out a proof of concept of just such a system with several banks.[23]

To be effective, however, blockchain-based KYC/AML registries would need harmonised regulatory requirements and standards across Member States. This is something that EU regulators will need to address.

Radical transparency can raise issues, too. Many market participants, unused to such transparency, may not feel comfortable with it at first. On the flip side, we can imagine that honest market participants might embrace such transparency, as it could dramatically reduce compliance costs, while fraudsters might find such transparency leaves them with fewer places to hide.

IMPROVING TRANSACTIONS, PROCESSES AND TRANSPARENCY IN PUBLIC AND PRIVATE-SECTOR MARKETS

In the previous section, we looked at how blockchain could help governments monitor and regulate markets in which they are not direct participants. In this section, we look at how blockchain might improve the ways in which governments transact and interact with citizens and companies directly, particularly in complex settings with multiple stakeholders and high transaction volumes.

Take tax and excise. Today, governments collect tax payments generally based on self-reporting by individuals and companies, with the threat of a future audit and potential sanctions one of the only ways of enforcing compliance. If, as we saw above, governments have access to market data at the transaction level, then they also, by default, have the information they need to calculate the tax liabilities of the parties to the transaction. This would theoretically help fight fraud and recover lost revenue. However, it also raises privacy issues and could be difficult to implement. A lot of effort goes into determining the correct level of taxation

[22] See for instance Blockchain application in supply chain chemical substance reporting, Sukhraj S. Takhar and Kapila Liyanage, 22nd Cambridge International Manufacturing Symposium, 27-28 September, 2018.
[23] Singapore regulator, OCBC, HSBC, MUFG create 'Know Your Customer' blockchain prototype, The Business Times, 3 October, 2017.

USE CASES: PUTTING BLOCKCHAIN TO WORK IN GOVERNMENT SERVICES

and this is a problem which cannot be solved by automation or smart contracts. Moreover, it is not necessarily in the interest of taxpayers, nor of governments, for tax authorities to gather so much data. In contrast, a registration system using data obfuscation methods like zero-knowledge proofs[24] can potentially be used to fight VAT fraud while ensuring that the tax authorities are only privy to the right data.[25] Though legally and operationally more complex and also problematic from a privacy perspective, by extension we could imagine similar platforms being devised to allow individuals and companies to automate much if not all of their tax calculations based on their transaction and financial data.

Governments are important actors in many large markets as well. We saw above how blockchain can be used to improve the handling of patient medical records. This could be used as a building block for governments to build blockchain-based platforms to improve the provision of government-sponsored healthcare, for example by automating insurance processes, better coordinating care, fighting waste through data sharing and reduction of redundant effort, and ensuring fairness in decisions about who receives care and when. The same could be done with the provision of social services, where with the help of digital identities, among other things, governments could automate payouts and more easily coordinate social services with other agencies, like departments of health or taxation or the police. Last but not least, blockchain-based platforms could conceivably improve the effectiveness and traceability of foreign aid, using smart contracts and other techniques to better ensure that funds reach their intended targets, and provide more reliable audits of how effectively aid has been employed.

Turning the tables, governments can use blockchains to improve their own processes, as well as provide more oversight and transparency. Blockchain-based systems could help governments get a better aggregate overview of their procurement processes and expenditures, for example by providing easy-to-access audit trails or making it easier for different agencies to share and aggregate data. Such data could then be made available to politicians and citizens, providing a much fuller picture of how tax receipts are being used. That in turn would give politicians and citizens better means to hold officials accountable for the wisdom and fairness of their spending decisions. Such platforms would also likely be welcomed by officials, who could benefit from a better overview of their spending, as well as from more automated processes and reporting capabilities.[26]

Blockchain-based shared ledgers and smart contract technology could also help streamline and improve the way governments interact with suppliers, for example by making procurement decisions more transparent. Smart contracts could also improve project oversight, with funds held in escrow on the chain and only paid out when contractors meet certain targets.[27] Automating payments would help governments with their own auditing, reporting and bookkeeping efforts as well. This, however, implies that governments are able put fiat currency on the chain, an interesting topic in its own right, and one we examine in more detail in the next section.

[24] Zero-knowledge proofs describe a set of methods for proving that a certain claim being made about the contents of a piece of data are true without revealing that data.

[25] See case study in Appendix.

[26] For more, see the YouTube video of the recent ECA conference on blockchain: opportunities and practical applications for EU expenditure control, European Court of Auditors (ECA) YouTube channel.

[27] This was addressed by the ECA, Op. Cit.

USE CASES: PUTTING BLOCKCHAIN TO WORK IN GOVERNMENT SERVICES

EFFICIENCY

As just implied, blockchain can help increase efficiency and reduce costs in government operations. These benefits can come from different quarters.

Whenever you digitise information, you generally gain efficiencies compared to paper-based processes. This is true for any digital technology. What makes blockchain interesting is the ability to digitise complex processes in a decentralised way with a distributed architecture.

Decentralised systems can be significantly more efficient than the traditional, centralised model for the simple reason that all users of the platform share the same infrastructure as opposed to each setting up their own siloed system. That means participants share the cost of implementing and maintaining the system, and can save on the expensive processes otherwise needed to reconcile data.[28] Distributed systems like blockchain tend to be very robust as well: since data is shared across the network, as long as at least one node remains functional, the data is secure. That can save costs on expensive backup and recovery systems. This is one reason why such an approach is favoured by the European Blockchain Partnership.

By facilitating the sharing of trustworthy data, blockchains could allow government agencies to share services more easily. As touched on variously above, agencies could share citizen identity data, saving them – and the citizen – the time and expense of continuously having to collect this information anew. By extension, blockchain should make it easier for governments to share data and services securely across borders, something of great import in a supra-national body like the EU. This could aid in implementing the "once-only principle" as enshrined in the European e-Government Action Plan 2016-2020,[29] which aims to reduce the administrative burden for citizens, institutions and companies in the EU by allowing them to provide certain kinds of standard information to authorities once, which the authorities can then re-use.[30]

FROM DREAMS TO REALITY

Thus, we have a picture of some of the ways blockchain technology could be used to enhance and transform how government services are delivered in Europe, increasing efficiencies, reducing costs and improving security along the way. These are all worthy goals, of course. They are also, at this point, aspirational.

In truth, there is still a long way to go before we will be able to implement many of these ideas. There are technological hurdles to overcome, from scalability and security of blockchains to the usability of the apps built on top of them. As we have pointed out elsewhere,[31] there are also many legal and regulatory questions still to be decided before blockchain-based platforms can be adopted on a mass scale. For a technology whose main purpose is collaborative data gathering and sharing, issues of data protection are among the most

[28] One example is sharing data on publicly held companies in Europe using blockchain, as envisioned by the European Financial Transparency Gateway pilot project. See The EU Is Building a 'Financial Transparency Gateway' with Blockchain, Coindesk, 11 August, 2017.

[29] European eGovernment Action Plan 2016-2020.

[30] For an overview, see EU-wide digital Once-Only Principle for citizens and businesses: Policy options and their impacts, DG CONNECT, 2017.

[31] Blockchain Innovation in Europe, EU Blockchain Observatory & Forum, 27 July, 2018.

USE CASES: PUTTING BLOCKCHAIN TO WORK IN GOVERNMENT SERVICES

important here.[32] Implementing blockchain for government services will also likely mean clearing political and bureaucratic hurdles.

In many use cases it may also be possible to get similar results without using blockchains at all. Should such solutions prove a more cost-effective or secure way to go, then they should by all means be considered. Like any technology, blockchain is simply a tool, not an end in itself. For this reason, experimentation needs to continue, including proofs of concept that weigh not just the technological feasibility of the solutions but also their economic and social impact. Recognising this, the European Commission has published a call for research proposals in its Horizon 2020 research and innovation programme to examine ways to reach this objective.[33]

[32] Blockchain and the GDPR, EU Blockchain Observatory & Forum, 16 October, 2018.

[33] See TOPIC : New forms of delivering public goods and inclusive public services

Foundations: key infrastructure for blockchain in government

For any technology to take hold it must have the right conditions. When looking at blockchain for government services, we have assembled a set of what we consider the most important enablers. These, it should be noted, are not just required to power blockchain-based government services. They are potentially critical to facilitate the emergence of both public and private innovation in Europe and to allow the development of a large-scale technology ecosystem.

IDENTITY: THE ESSENTIAL PREREQUISITE

One of the most important requirements in building a digital economy and society is viable digital identities for all participants, whether individuals, companies, public agencies or, increasingly, machines and other autonomous agents. The need to be able to identify ourselves and others is so important, in fact, that it is considered the essential prerequisite for most use cases.

To be able to truly benefit from the potential of blockchain technology for the provision of services, governments will need to develop digital identity systems that can be used in blockchain-based platforms. In doing so, they could, at the same time, address some of the broader problems with digital identity in our world today.

For all its miraculous properties, our most important global online platform – the internet – has no built-in identity mechanism. As a result, online identities are "provided" to individuals by a heterogeneous mix of more or less trustworthy sources. Traditional authorities like governments, utilities or banks continue to provide important verifications of who people claim to be. But key identity information about individuals is increasingly in the hands of those who own the online services they use, like social media, e-commerce or news sites, or those who have surreptitiously gathered information about people for their own ends.

While, for lack of an alternative, this paradigm has worked so far, it is by no means ideal. It leaves the average person with hardly any control over what happens to his or her own data. It also leaves that data highly exposed, as we learn through the almost daily reports of hacks and breaches. Online identities today are also easily forged, reducing trust. Even if safe, today's paradigm – with bits and pieces of identity information saved in hundreds if not thousands of databases in all corners of the internet – is terribly inefficient and not user-friendly.

Governments are aware of this problem, and many are taking measures to address it. In Europe we have the GDPR,[1] which aims to protect personal data online, and the eIDAS,[2] which aims to set legal and technical standards for digital identification and signatures with an eye to making them interoperable across borders.

[1] General Data Protection Regulation.

[2] Regulation on electronic identification and trust services for electronic transactions in the internal market.

FOUNDATIONS: KEY INFRASTRUCTURE FOR BLOCKCHAIN IN GOVERNMENT

Blockchain offers the possibility of a more fundamental fix to the digital identity problem based on turning the current paradigm on its head. We refer to “self-sovereign” identity and believe that governments pursuing the use of blockchain should make this a cornerstone of their strategy and look to become important contributors and facilitators to viable self-sovereign identity solutions.[3]

Blockchain-based self-sovereign identity is based on the idea that, instead of having identity information on individuals kept by third parties, individuals would be able to keep verified identity information themselves. In the self-sovereign paradigm, governments could, for instance, issue digitally signed certificates to their citizens or residents attesting to the person’s name, address, birth date, place of residence, ability to drive a car, land title, voter registration and so on. This person could then present these credentials as and when needed, similar to the way people use physical identity documents like passports and drivers’ licences today. Because blockchain makes it easy to verify the authenticity of the information provided, as well as of the authority that is being relied upon, such credentials could in theory be far more trustworthy and secure than the physical variety, which can easily be forged or stolen.

While the details of how self-sovereign identity functions are beyond the scope of this paper, the concept has been avidly discussed since the early days of blockchain and continues to garner great attention. Yet getting self-sovereign identity to work on a government level will be a challenge on many fronts.[4]

Of these, perhaps the most pressing will be developing the necessary identity standards. Defining a clear identity framework and how it could work in a more decentralised way is an effort being carried out by organisations such as the Decentralized Identity Foundation[5] and the W3C.[6] Decentralised Identifiers (DIDs) and verifiable credentials[7] are the first steps toward interoperable systems.

There will be important architectural decisions as well. To what extent do we want self-sovereign identity systems to be decentralised, or can we accept a certain amount of centralisation? Where should identity data be stored and who should have access to it? While the idea of having full control over identity data sounds good in theory, it also carries with it grave responsibilities. Under the self-sovereign paradigm, individuals are, at least in theory, responsible for safeguarding their own identity data. They will need to be made clearly aware of what that means and educated in how best to protect themselves. We will also likely need to develop safeguards, for instance ways for people to recover their identity data should they lose their devices or passwords.

The self-sovereign paradigm also raises a number of privacy and refutability issues. What happens to those with legitimate reasons for wanting to act anonymously online? A particularly thorny issue in Europe – and one which we touch on below, as well as in a dedicated paper[8] – is how to reconcile the immutable nature of blockchain-based identity information with the data protections enshrined in the GDPR.

[3] By providing a pan-European standard for digital signatures, eIDAS can be one important cornerstone.

[4] The EU Blockchain Observatory & Forum will be publishing more focused reports specifically on the topic of identity.

[5] Decentralized Identity Foundation.

[6] See https://w3c-ccg.github.io/did-spec/: “Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, ‘self-sovereign’ digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority.”

[7] See https://w3c.github.io/vc-data-model/.

[8] Blockchain and the GDPR, EU Blockchain Observatory & Forum.

Governments will also want to take care how they design blockchain-based digital identity platforms. They will have to take into account how identity attributes change over time during a person's natural lifecycle, and will need to offer different levels of transparency depending on the context (e.g., verifying that someone is over 18 without providing a birth date).[9] Identity platforms also need to be inclusive of all citizens, including those who, for whatever reason, have no access to or are not able to use technology. That raises important legal and regulatory issues around, for example, digital guardianship.

BLOCKCHAIN PLATFORM AS A SERVICE: THE RIGHT TOOLKIT

If governments want to successfully deploy blockchain technology for themselves, they will, of course, need the requisite infrastructure. This will be challenging with a technology as new as blockchain, one that is evolving rapidly and for which there are still few standards or clear examples of best practice.

In deciding which way to go, we think there are many factors that governments should keep in mind. They will want, of course, to evaluate the costs involved. An ideal platform should also be easy for various government agencies to use for their own ends and also be conducive to data sharing and creating interoperable processes across agencies. There are also pitfalls they should avoid. While experimentation is good and should be encouraged, it can be easy to lose precious time and money in long cycles of use case identification, proof of concept building and vendor selection. This problem is compounded if government agencies work on their own, siloed blockchain solutions instead of working together on a single approach. For the same reason, governments should be careful to ensure that experience with and expertise in blockchain is shared among agencies so that all can profit. These concerns and opportunities are addressed through the EU Blockchain Services Infrastructure by the Member States and the European Commission as part of the European Blockchain Partnership.

There are different ways to solve these problems. A government could decide to take a top-down approach, developing one blockchain platform for all agencies and mandating its use. This can serve the cause of standardisation but runs the risk of not being adequate to meet the real needs of the agencies, or locking the government into a single vendor or technology and hence potentially missing out on new developments. Governments could also let their agencies experiment and build blockchain platforms themselves, but that runs the risk of fragmentation of platforms and knowledge, creating a whole that is less than the sum of its parts.

We think a promising way forward that strikes a middle ground between these two extremes is the Blockchain Platform as a Service model (BPaaS). This is basically a flexible, cloud-based shared infrastructure that hosts different protocols as well as developer tools, and an integrated development and operations environment. This would allow agencies to relatively quickly evaluate and choose preferred technology, build proofs of concept and test the results.

Such an approach has many advantages. It should be easier and faster, and, more importantly, less costly, than using dedicated

[9] Such concerns are addressed by eIDAS. See What's the Difference Between Advanced and Qualified Signatures in eIDAS?, GlobalSign, 21 March 2017.

internal IT departments or individual vendors chosen through lengthy RFP processes. Adoption will likely be sped up by reducing the time lost to trial and error: with the ability to quickly and flexibly explore blockchain solutions, agencies can quickly learn what works and also what doesn't, without costly up front investment. A shared "sandbox" approach, even one featuring multiple technologies, should also foster knowledge sharing and make it easier for agencies to work together to ensure interoperability.

TOKENISED FIAT CURRENCIES: MONEY ON CHAIN

A large percentage of government services involves monetary transactions of some sort. By their very nature, blockchains are excellent transaction platforms. But in order to reap their benefits, and, in particular, real-time automation of payments through smart contracts, governments will have to find a way to make it possible to carry out these transactions in the national currency directly on the chain.

This can be done in a number of different ways. Some central banks have been looking at tokenising national currencies to create, in effect, fiat cryptocurrencies, referred to as central bank digital currencies (CBDC).

One of the most widely watched early trials of the idea has been Project Ubin in Singapore, which is being spearheaded by the Monetary Authority of Singapore (MAS) with a consortium of banks and technology companies. The project has been focusing on inter-bank payments with distributed ledgers, but aims to explore in full the potential of tokenised central bank money to help make financial transaction processes more transparent, resilient and cost efficient, for example through immediate settlement of transactions.[10] Similar projects have been carried out in South Africa,[11] Russia[12] and between the UAE and Saudi Arabia.[13]

In Europe, the Bank of England, which made waves several years ago as one of the first central banks to begin looking at blockchain for fiat currencies,[14] has continued with a concerted research effort into the subject and recently released a paper on design principles for central bank digital currencies in general.[15] The Swedish Riksbank has also carried out a project looking at a potential e-krona.[16]

While none of these central banks has plans to issue digital versions of their fiat currencies at the moment, the idea is interesting for several reasons.

Putting digital versions of national currencies on the blockchain means they could then become integral parts of smart contracts. That would unlock much of the potential innovation of blockchain by allowing parties to create automated agreements, including direct transactions in these currencies, instead of having to use a cryptocurrency as a proxy.

On a systemic level, central bank digital currencies could, among other things, bring

[10] Project Ubin: Central Bank Digital Money using Distributed Ledger Technology, Monetary Authority of Singapore.
[11] South Africa's Central Bank Claims Success in Blockchain Payment Trial, Coindesk, 6 June, 2018.
[12] Regional Government in Russia to Test Blockchain Payments, Coindesk, 20 February, 2018
[13] UAE and Saudi Arabia Collaborate on Central Bank Digital Currency Research, nulltx.com, 16 December, 2017
[14] The economics of digital currencies, Bank of England Quarterly Bulletin 2014 Q3.
[15] Digital Currencies, Bank of England.
[16] E-krona, Sveriges Riksbank.

the benefits of decentralisation to inter-bank payments and real-time gross settlement systems (the systems used to "finalise" transactions, which is known as "settlement" and can be a very complex process). These benefits include resiliency and security, increased efficiency and cost savings, all while (if desired) preserving privacy and/or increasing transparency.

Payment is not the only use case for central bank digital currency, however. Central banks are also considering it as a means to issue digital cash to citizens (as an adjunct to or replacement for physical bank notes), and as a way to add additional tools to the monetary policy toolkit. All of these use cases are compelling for various reasons, but also contain a number of risks and uncertainties.[17] We therefore should not expect a widespread movement toward central bank money on blockchains any time soon. When and if it comes, however, we believe it does have significant potential in many areas.

Governments could potentially use blockchain-based tokens in non-monetary ways as well, for example as a type of e-voucher that can be exchanged for government services. Such vouchers could be issued as rewards for community-oriented behavior, for example, like recycling or offering surplus energy from your home back to the neighborhood.

POLICY AND REGULATION: RULES FOR THE CHAIN

As we have seen, blockchain introduces many new paradigms and potential business models, often through the mechanism of decentralisation. These naturally bring up various regulatory and policy issues.

On the policy front, the most important impact that government agencies can have is by driving adoption of the technology, which can be accomplished by launching projects themselves or sponsoring public/private partnerships. One example of such a project is the UN's ID2020 initiative,[18] in which the UN is working with corporate partners to provide formal identities to the more than one billion individuals on the planet who do not have one, including millions of refugees.

We have seen this for example in Dubai[19] and the above-mentioned Project Ubin in Singapore. In Europe, where there is keen interest in blockchain on the part of EU bodies and national governments, we are also seeing a growing number of such public/private projects, for example the Vehicle Wallet partnership between a payment service provider and the Danish Tax Administration.[20]

With its long tradition of public-private partnerships, such efforts play to Europe's strengths.[21] Because it is a technology suited to building large electronic markets, it is natural in many cases to form industry-based or geographic consortia, as we have seen, for example, with the MOBI effort in the automotive industry[22] or Alastria,[23] which is building a national blockchain platform for

[17] Central bank digital currencies, Markets Committee, Bank for International Settlements, March 2018.

[18] id2020.org

[19] See the Dubai Blockchain Strategy.

[20] Blockchain-powered eWallet to Automate Payments in Smart Cars, Future-Car, 2 February, 2017.

[21] In this regard, the EU Blockchain Industry Roundtable of 20 November was organised by the European Commission with a view to launching an international alliance and association (International Association for Trusted Blockchains Applications).

[22] dlt.mobi

[23] alastria.io

businesses and the public sector in Spain.[24] Governments can do a lot to support this technology by joining and/or facilitating such efforts.

Blockchain also raises a number of regulatory issues that governments will need to address.

As already mentioned, and as we examine in detail in a separate paper, perhaps the most important blockchain-related regulatory issue of the moment is how to square blockchain with many of the data protection provisions contained in the GDPR.[25] In other cases, we have seen how blockchain-based platforms clash with local or more mundane issues of law. The Swedish Land Registry project mentioned above, for instance, will remain a pilot for the time being for the simple reason that, in Sweden, the contracts for the transfer of land title must, for legal reasons, be done on paper.

The more general question of the legal status of smart contracts is also an essential part of the overall blockchain discussion. There are many open questions as to the legal validity of such contracts, often lumped together as one overriding question: "can code be law?" Issues here include how to enforce the stipulations of a smart contract on a blockchain with its real-life counterparts, how to handle litigation and appeals in automated, self- executing agreements, as well as what to do if there is a flaw in the code, as famously happened with the Ethereum DAO.[26] Considering blockchain's "notary" properties, we can also ask to what extent blockchain records are legally binding.

Another important question revolves around the need, if any, to adopt new legislation to define liabilities when using blockchain. To what extent do we need to clarify and/or adapt current frameworks (e.g. modifications that should potentially be made to eIDAS to account for opportunities created by blockchain)? To what extent do we need to write new rules to take into account specific use cases?

These questions are being investigated. For instance, the EU Commission is analysing existing obstacles in legislation with regard to the rise of new technologies and their uptake, especially for artificial intelligence, IoT and blockchain. This is also an exercise the EU Commission is bringing forward internally across all its departments. The EU Blockchain Observatory & Forum, for instance, will be dedicating an upcoming workshop to highlighting existing regulatory obstacles or missing legal frameworks as identified by a wide community of stakeholders.[27]

[24] Spanish Autonomous Community of Aragon to Become First in Country to Apply Blockchain, Cointelegraph, 17 September 2018.

[25] See Op. Cit., Blockchain and the GDPR, EU Blockchain Observatory & Forum, 16 October, 2018.

[26] Blockchain Innovation in Europe, EU Blockchain Observatory & Forum, 27 July, 2018.

[27] Workshop on Blockchains & Smart Contracts Legal and Regulatory Framework, Paris, 12 December, 2018.

Looking ahead: priorities and recommendations

In this report, we examined the potential of blockchain technology for improving government and public services. We would like to close by considering some of the measures Europe can take to implement these use cases.

The first step is to set up the right infrastructure to make sure it is easy and fast for government agencies and institutions to build their own applications in a cost-effective and interoperable manner. As we outlined above, this infrastructure is based on three foundations: viable digital identity (in our opinion, of the self-sovereign kind); a cloud infrastructure that can accommodate and scale at the required rate, also called blockchain platform-as-a-service; and tokenised fiat currencies to bridge the gap between blockchains and banking systems and unfold the benefits of automatic payments powered by smart contracts. While setting up the right infrastructure is a real challenge, there are many experiments and implementations that could be a source of inspiration.

Second, the ecosystem would benefit from tailored policies and regulations, clarifying and adapting current frameworks when relevant and implementing new rules if required. Regulations covering legacy systems have a lot of room for improvement, as they were conceived at a time when blockchain technology had not yet appeared. Possible adjustments or clarifications to regulations such as eIDAS and its implementing acts should be studied in detail to identify if there is a need to adapt in order to account for the opportunities created by blockchain. The same can be said about potential clarifications of the GDPR with respect to blockchain. On the other hand, blockchain technology is creating new opportunities by disrupting entire industries and creating new business models. These do not always fit well into existing regulatory frameworks, raising the question of whether these frameworks need to be adapted to blockchain's new realities. In Sweden, for instance, one hurdle to implementing the blockchain land registry is a law that states that the contracts for transferring land title deeds must be on paper. While blockchain is, by nature, one of the most trustworthy notary services available, it will be useless if the law doesn't recognise blockchain-notarized data. Legal harmonisation between Member States will also be crucial if we want to see the implementation of cross-border use cases.

Third, educating the general public, entrepreneurs and civil servants should be a priority. Helping these actors understand the benefits of the technology, envision potential use cases and develop blockchain-based solutions is decisive for the broader adoption of the technology. Current systems will be upgraded and new services created only if the people involved are given the right tools and training. Blockchain and other emerging technologies may also lead to a certain number of job redundancies, which will require people to be retrained. On the other hand, as a burgeoning industry in its own right, blockchain will be a source of new employment opportunities as well.[1]

[1] Many of these jobs will be technical, but not all. See: What are some jobs that the blockchain technology will create?, Quora, 26 September, 2018.

LOOKING AHEAD: PRIORITIES AND RECOMMENDATIONS

Fourth, the EU should take the opportunity to drive high-impact projects through Member States and public/private collaboration, as well as dedicated research and development. Taking a leading position could accelerate the development of the broader ecosystem while directly benefiting citizens. Moving toward the definition of industry standards nurtured by knowledge transfer facilitates future interoperability. Sharing learnings and best practices that could benefit the whole ecosystem acts as a catalyser. Collaboration on research is also very important given the nascent status of blockchain technology. Providing impulse to projects could be done by using existing European funding mechanisms, but also by encouraging the development of cross-border projects between Member States. Europe should also continue to support research into the technology, as well as other important areas of best practice. In particular, network governance in large-scale decentralised systems is still not well understood. To make decentralised systems work, those who build them and those who use them will need to gain and share experience of how they work. Last but not least, European governments should keep in mind that neither they nor blockchain act in a vacuum. Public/private collaboration, particularly through consortia, should be encouraged wherever it makes sense, and the conditions set to make it easy to build and implement them.

Appendix: case studies

CASE STUDY 1: SWEDISH LAND REGISTRY

The Lantmäteriet is the Swedish mapping, cadastral and land registration authority. Although the real estate transfer process works quite well in Sweden, the authorities were interested in finding out if it could be improved with blockchain, in particular by making it faster, more transparent and less costly. To that end, the Lantmäteriet collaborated with banks, the tax authorities, blockchain developers and some other stakeholders to map the real estate transfer process on the blockchain (not the transfer of title) and subsequently used this map to complete a successful proof of concept for such a transfer.

The solution is a private blockchain developed especially for the project. The goal is to provide technical verification of the data and the transactions. The nodes do not vote on the transactions but merely see to it that the protocol is followed. The incentive to create blocks lies in the parties' business models and legal demands that drive the process of selling real estate through to the point where the transaction is registered in the land registry.

Users of the platform employ e-signatures (such as Telia ID) to sign documents online in the contract engine. The contracts are then validated by the nodes on the network and stored offline in a separate database. When all necessary steps have been taken and validated, the bill of sale goes to the land registry (which is not on the blockchain). While contracts are stored off-chain – for GDPR reasons, among others – certain personal data that is required to be made public in a real estate transaction in Sweden is released in the early stages.

While there are currently no plans to implement the system in a live setting – a contract to sell property in Sweden needs by law to be on paper and not digital – the project has gained a lot of attention as a test case for blockchain in government, as well as a source of important learning.

CASE STUDY 2: VAT SYSTEMS

In Europe, Value Added Tax (VAT) is an important source of revenue for Member States and the European Union. It is also a system facing many challenges.

Every year, some €150 billion is lost annually to VAT fraud.[1] Much of this can be traced back to the fact that VAT needs to be self-reported. While tax authorities can audit returns after the fact, the process is expensive and slow, meaning only a small fraction of returns is actually examined.

Dutch startup summitto[2] is building a blockchain-based platform that aims to combat VAT fraud. The solution relies on confidential time-stamping of every invoice and the provision of aggregate invoice data to the tax authorities. As a result, and assuming the majority of the companies in a country honestly report their invoices, at the end of the month the tax administration can easily identify the likely dishonest actors.

The solution is based on a permissioned blockchain that contains a confidential, time-stamped registry of invoices, bringing transparency but also efficiency to the VAT process. Its solution, the company says, will improve fraud detection but also allow for that automation of VAT reporting.

CASE STUDY 3: BLOCKCHAIN IN ESTONIA

Estonia has long been a pioneer in e-government, and this has continued in the age of blockchain. After starting to test the technology back in 2008, Estonia became the first nation state to deploy blockchain technology in a production setting with its Succession Registry (wills) in 2012.

Estonia uses Guardtime's KSI blockchain, which is a permissioned blockchain technology. The blockchain is used primarily for data integrity assurance: if a public organisation has a digital asset, it can use the blockchain-backed service to compute a hash of this asset (e.g. a health record) to give it a unique digital fingerprint. This hash is then sent to the

[1] VAT: EU Member States still losing almost €150 billion in revenues, European Commission, 21 September, 2018.
[2] summitto.com

APPENDIX – CASE STUDIES

blockchain, which returns a proof of registration (KSI signature) to the user of the service. The user or any other third party, for example a citizen or an auditor, can, in turn, use this to identify the asset's integrity, the signing time and the signing entity without relying on a third or a trusted party.

In this way, no actual data goes to the blockchain, which means there are no privacy issues, making the system fully compliant with strict data protection regulations. The blockchain is used to provide an independent root of trust and immutability: a piece of information that is linked with the blockchain can be trusted not to have been modified at any point.

It is also used for creating trust in different e-governance services. In Estonia, citizens can log in to the system at any time and see who has handled their data (for instance to see if the police have run their licence plate or a doctor has handled their medical data). The blockchain solution is designed to make sure that everything has been securely logged and not tampered with by malicious insiders or outsiders.

KSI blockchain is being used in Estonia by a number of ministries and public state registries. For example, Estonia has an e-health registry backed by blockchain which can be used for paperless prescriptions. The blockchain integration assures and provides independent proof of the integrity of both personal health records and their processing. Estonia also uses blockchain for managing digitised paper records (for example wills). All legislation that is published in the Estonian State Gazette is also registered on the blockchain, providing indisputable proof of each law's state in time. Other projects being looked at include: government cloud, quantum immune ID scheme, connected vehicle incident handling programme (relevant to self-driving cars) and research on distributed registries.

Appendix – Blockchain Terminology

What is a blockchain?

Blockchain is one of the major technological breakthroughs of the past decade. A technology that allows large groups of people and organisations to reach agreement on and permanently record information without a central authority, it has been recognised as an important tool for building a fair, inclusive, secure and democratic digital economy. This has significant implications for how we think about many of our economic, social and political institutions.

How does it work?

At its core, blockchain is a shared, peer-to-peer database. While there are currently several different kinds of blockchains in existence, they share certain functional characteristics. They generally include a means for nodes on the network to communicate directly with each other. They have a mechanism for nodes on the network to propose the addition of information to the database, usually in the form of some transaction, and a consensus mechanism by which the network can validate what is the agreed-upon version of the database.

Blockchain gets its name from the fact that data is stored in groups known as blocks, and that each validated block is cryptographically sealed to the previous block, forming an ever-growing chain of data. Instead of being stored in a central location, all the nodes in the network share an identical copy of the blockchain, continuously updating it as new valid blocks are added.

What is it used for?

Blockchain is a technology that can be used to decentralise and automate processes in a large number of contexts. The attributes of blockchain allow for large numbers of individuals or entities, whether collaborators or competitors, to come to consensus on information and immutably store it. For this reason, blockchain has been described as a 'trust machine'.

APPENDIX – BLOCKCHAIN TERMINOLOGY

The potential use cases for blockchain are vast. People are looking at blockchain technology to disrupt most industries, including from automotive, banking, education, energy and e-Government to healthcare, insurance, law, music, art, real estate and travel. While blockchain is definitely not the solution for every problem, smart contract automation and disintermediation enable reduced costs, lower risks of errors and fraud, and drastically improved speed and experience in many processes.

Glossary

The vocabulary used in the context of blockchains is quite specific and can be hard to understand. Here are the essential concepts you should know in order to navigate this breakthrough technology:

- **Node:** A node is a computer running specific software which allows that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network.
- **Signature:** Signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography allows someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key.
- **Transaction:** Transaction are the most granular piece of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that transaction content has not been manipulated while being transmitted over the network.
- **Hash:** A hash is the result of a function that transforms data into a unique, fixed length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data.
- **Block:** A block is the data structure used in blockchains to group transactions. In addition to transactions, blocks include other elements such as the hash of the previous block and a timestamp.
- **Smart contract:** Smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus leveraging

APPENDIX – BLOCKCHAIN TERMINOLOGY

the trust and security of the blockchain network. They allow users to automate business logic and therefore enhance or completely redesign business processes and services.

- **Token:** Tokens are a type of digital asset that can be tracked or transferred on a blockchain. Tokens are often used as a digital representation of assets like commodities, stocks and even physical products. Tokens are also used to incentivise actors in maintaining and securing blockchain networks.
- **Consensus algorithm:** Consensus algorithms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means depending on the specific needs. The most famous consensus algorithms include Proof-of-Work, Proof-of-Stake and Proof-of-Authority.
- **Validator nodes:** Validator nodes are specific nodes in a network that are responsible for constituting blocks and broadcasting these blocks with the network. To create a valid new block they have to follow the exact rules specified by the consensus algorithm.

Learn more about blockchain by watching a recording of our Ask me Anything session.