Evidence Report
APPG BLOCKCHAIN
UK Parliament

appg

ALL-PARTY
Parliamentary
Group on
Blockchain

HOW CAN BLOCKCHAIN HELP IN THE TIME OF COVID-19?

NATIONAL SECURITY

Blockchain applications - regulation, policy & strategy

2020 JUNE

BIG
INNOVATION
CENTRE

Sponsors of APPG Blockchain

The Group supporters – Big Innovation Centre, British Standards Institution, Capita, CMS Cameron McKenna Nabarro Olswang, INDUSTRIA, IOTA Foundation, MyNextMatch, PubliQ and SAP – enable us to raise the ambition of what we can achieve

www.biginnovationcentre.com | info@biginnovationcentre.com | @BigInnovCentre
www.appg-blockchain.org | appg-blockchain@biginnovationcentre.com | @appg_blockchain

Table of Contents

1. APPG Blockchain Evidence Meeting: National Security & The Fight Against COVID-19.

1.1. Purpose

The mission of the All-Party Parliamentary Group on Blockchain (APPG Blockchain) is to ensure that industry and society benefit from the full potential of blockchain and other distributed ledger technologies (DLT) making the UK a leader in Blockchain/DLT's innovation and implementation.

This is an Evidence Report of an APPG Blockchain Evidence Meeting which explored the potential of Blockchain and DLT on National Security and how Blockchain Technology can be used in the fight against COVID-19.

The first part of the meeting focussed on the uses of Blockchain for Digital Identity, as well as the approaches of the European Union and Estonia Government in this respect. The second part reviewed, Blockchain use-cases and applications to support the current fight against the COVID-19 pandemic.

This report provides a summary of the takeaways from the meeting. The Video recording of the meeting is available on our websites APPG Blockchain *https://www.appg-blockchain.org/* and Big Innovation Centre *https://www.biginnovationcentre.com/*

1.2. Details

- Date of meeting 08 April 2020
- Time, 17:30 – 19:00pm BST
- Location moved from UK Parliament to Webinar due to the UK Covid-19 lockdown
- Participants, 109 attendees

1.3. Panellists: Evidence Givers, Chair & Secretariat

The meeting was Chaired by APPG Blockchain Chair Martin Docherty-Hughes Member of Parliament. Parliament has appointed Big Innovation Centre as the Secretariat for the APPG Blockchain, led by CEO, Professor Birgitte Andersen.

The webinar brought a total of 7 evidence givers from 5 different countries (Canada, Estonia, Spain, the United Kingdom and the USA).

Figure 1: Panellists

Evidence givers on National Security, Digital Identity & COVID-19

Taavi Rõivas, Estonian MP & Former Prime Minister, Estonian Parliament *(Estonia)*

Angel Martín, Spanish representative in European Blockchain Partnership, Ministry of Economic Affairs & Digital Transformation *(Spain)*

Geoffrey Goodell, Senior Research Associate, UCL Centre for Blockchain Technologies *(UK)*

Evidence givers on Blockchain Applications & COVID-19

Don Tapscott, Chairman and co-Founder, Blockchain Research Institute (Canada)

Marta Piekarska-Geater Director of Ecosystem, Hyperledger *(UK)*

Andrew Tobin, Managing Director EMEA, Evernym Inc *(UK)*

Jonathan Levi, Founder, HACERA & Unbounded Network *(USA)*

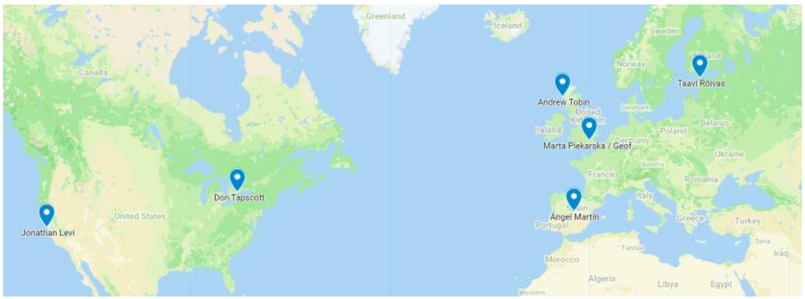
Chair, Vice-Chair and Secretariat

CHAIR: Martin Docherty-Hughes, MP, UK Parliament

VICE-CHAIR: Lord Waverley House of Lords, UK Parliament

Secretariat: Professor Birgitte Andersen, CEO, Big Innovation Centre *(UK)*

Figure 2: Speakers from around the World.



1. Summary

1.1. Main takeaways

The current global health crisis is a turning point for our entire socio-economy and way of life. It has demonstrated problems in our systems for innovation, procurement supply-chains, data governance, and our entire technology infrastructure and society.

Blockchain has become the new multi-purpose technology, - not only an urgent tool in the fight against COVID-19 pandemic, but also to unleash trade, investment, and future finance for the economy. There are lessons for national security as well.

But what does good look like?

Questions for Discussion at the meeting were:

National Security

- What does digital identity mean for transparency, anonymity, and freedom?
- Does blockchain aid cybersecurity?

Fight against COVID-19

- How can Blockchain support the current fight against COVID-19?

Below we have summarised the key takeaways from the session. The evidence presentations are listed in the subsequent sections.

Figure 3: APPG Blockchain Webinar 8 April 2020

Figure 4: Overview

TAKEAWAYS	EVIDENCE SNAPSHOTS
A radical approach is vital: Radical innovation to our data infrastructure is needed throughout the economy (as opposed to fixing technologically redundant systems) if we want to bounce back from the current economic, business, social crises, including our health care responses to COVID-19. Blockchain, has proven merit.	***Taavi Rõivas*** *explains how Estonia is built as a digital nation since it became independent in the early 1990s, including all the details of the country's institutions and information systems. Encrypted databases called 'hash linked time stamping' were innovated and adopted before the technology emerged into Blockchain technology as we know it today. Since 2008, Estonia adopted e-health and the healthcare registry has since operated on a blockchain (alongside other data registries, such as those related to property, business and succession registry).*
Decentralised, autonomous, self-sovereign identity Blockchain systems should be adopted: • They provide safe control to people on how their data are used. • They allow the health sector to protect electronic records of patients into cases of sensitive diseases. • Finally, such systems allow (in principle) users to trace the interactions with people diagnosed with the disease, in a privacy-preserving and secure way. • Other Blockchain applications of this kind for the health care sector include tracing, tracking, and controlling vaccinations, prescriptions, medical records, health insurance, drugs, and infections on people.	***Marta Piekarska-Geater*** *presents evidence and use-case from HIV infected communities, on how there is already space, need and uptake of decentralised autonomous self-sovereign identity systems, made possible by Blockchain. That is where data belongs to the user, or the humans, or the devices, rather than centrally controlled Authority****.*** ***Angel Martin*** *explains how 'digital credentials' in self-sovereign identity blockchain model under the control of the individual, means increased privacy, improved interoperability without a central database, and can operate safely with a cross-border dimension.*

There is a need for Digital Verifiable Credentials:

We need digital versions of the credentials which can be used globally. Credentials need to be interoperable and verifiable a. It is not just about identity.

- Credentials could be anything that conveyor certification and entitlements or achievement, and they all need to work online as well.
- They are needed for all trusted systems and to increase the mobility of health workers and other people or things.

***Andrew Tobin** argues how the Covid-19 pandemic is the catalyst for massive acceleration to solve the digital trust problem, i.e. trust at a distance.*

Commodification of data could be an option to unleash solutions for the health crises and technological unemployment:

- Through a Social Contract (revenue incentives for data sharing), the commodification of data delivers the raw materials (i.e. data) and foundation for COVID-19 research, and it enables blockchain adoption for the tracing and tracking of pandemics.
- Finally, it can support life wages (guaranteed universal basic income) to citizens during a period of crises and while technology is substituting many of their jobs.

*Most urgently, we need public and private incentives for data sharing. **Don Tapscott** argues that the time may be ripe for guaranteed universal basic income to citizens, as part of a Social Contract in which they share their data for public and private purpose.*

Decentralised autonomous self-sovereign identity systems have security limitations unless certain conditions are in place:

For blockchain designs, we must consider the balance of power between the individual versus the state or the big tech companies. Also, we must consider the danger of hacking:

- Blockchain cannot, or should not, be used if cannot make the data fully private.
- Blockchain systems should allow for multiple identities of individuals (as opposed to one Master Root Identity)

***Taavi Rõivas**, argues that safety is important and blockchain cannot, or should not, be used to store personal data (only hashtags).*

***Geoffrey Goodell** challenges alternative blockchain designs and argues how credentials of people must not be linked (e.g. to one Master Root Identity) on the Blockchain. Instead, he advocates for the use of systems allowing for multiple identities to ensure the people's control over their data, and better security.*

*This was also the view of **Jonathan Levi,** who emphasised the problem of data triangulation which should be avoided. He argues how the biggest problem that we have is privacy, and especially in a crisis mode in an emergency government or in any jurisdiction, people forget this one thing.*

Create an Emergency Task Force on medical data:

1. **Governments can be a model user of the technology, where governments** can focus on the supply side for market data, not just the demand side.
2. Governments are the world's largest supply chains they should be using this technology for their supply chains piloting cases

it means

3. **passing legislation** to mobilise stakeholders around
4. creating **self-sovereign** identities and citizen-owned health records

they should

5. pilot blockchain and incentive systems for motivating people and having them behave responsibly

*As a forward-thinking agenda, **Don Tapscott** advocates every national government to create an emergency Task Force on medical data to start planning and implementing blockchain initiatives. It can stimulate the development of technology firms working on the solutions through all kinds of ways*

6. partner with medical professional associations and other players to implement blockchain-based credential systems
7. central banks should move quickly and swiftly to create **Fiat digital** currencies in their country, and the IMF should take a leadership role in rolling these **up to a global synthetic hegemonic cryptocurrency.**

Build ecosystems for Blockchain solutions to generate a single version of the truth and coordinate action:

The ecosystems parts to be crowded-in to be working together include:

- Trusted data capture (e.g. WHO [World Health Organization], ECDC [European Centre for Disease Prevention and Control]) and distributed data storage
- Model builders and data analysts (university research people and institutions)
- Top cloud providers and Big Techs.
- Hackathons have proven useful as well.

***Jonathan Levi** explains that successful Blockchain implementation to various use-cases (including for COVID-19 and related trusted tools analytics and applications) requires a trusted ecosystem coordinator.*

2. Evidence Giving

2.1. Don Tapscott, Chairman and co-Founder, Blockchain Research Institute (Canada)

Feature: Don Tapscott argues how the current global health crises is a turning point for the world as we see it today. It has demonstrated problems in our systems for innovation, identity, commerce data, and our entire technology infrastructure. Blockchain has become the new multi-purpose technology, - not only an urgent tool in the fight against COVID-19 but also to unleash the supply chains and future finance of the economy. Most urgently, public, and private incentives for data sharing and a government-led Emergency Task Force on Medical Data is needed to unlock the immediate crises.

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence giving: Don Tapscott

It is a real delight to participate in this important conversation, and governments are obviously quite central to us moving forward. You know the view of the old leaders Margaret Thatcher and Ronald Reagan that “the best government is no government”. I think being a libertarian of that sort, is maybe an unpopular thing these days, as people understand that the state is actually important.

I have co-founded the blockchain research institute *(www.blockchainresearchinstitute.org),* and I have been at this whole digital thing for a long time dating back to the 1970s when I was at Canada's Bell Labs Bell-Northern Research.

I think this is one of ***those rare turning points in history that this pandemic will bring about, is profound changes to our economy or behaviour in our society,*** and you know some leaders that fail the challenge will be replaced. Many institutions will be scrutinised and hopefully, change for the better.

> *In these uncertain economic times, blockchain-based identity solutions provide the framework for building in incentives for data sharing, where individuals can co-create value from the very data they generate, and be part of a new kind of solution, be it a cure to a rare disease or greater control protocols to mitigate the spread of a deadly virus.*
>
> *The issue of overcoming challenges to the implementation of these solutions remains a question of leadership.*

The pandemic has revealed some very deep **problems in our systems for innovation, identity, commerce data, and our entire technology infrastructure.**

And this got a lot to do with data or lack of data.

1. Obvious to clinicians' epidemiologists, there is have been virtually no testing in the early weeks of the outbreak in most Western countries
2. Supply chains have proven inadequate failing to respond to the need to produce something as simple as a paper mask and
3. Consumers lacking transparency become fearful they have hoarded basic staples (lack of food supply and other basic items).

There is a big question on the table to how can such situations be avoided in the future? But right now, immediately, how can blockchain be used to help us move forward?

We have a big program right now on blockchain in public health and a focus on blockchain and pandemics. Yesterday we published a very significant report (25,000 words) available at *www.blockchainresearchinstitute.org/blockchain-and-pandemics*. I would like to use this to set up the framework for the conversation, the second era of the digital age.

Insofar as you know, machine learning, the Internet of Things and all this other exciting technology that is coming on board, is going to be pertinent to our economies or governments or society. **It will need a transactional platform, and to me blockchain is at the heart of**

that. A number of the topics have been raised in this very thoughtful conversation, so let us begin up at the top with:

Supply chains

Supply chains is now a trillion-dollar industry and blockchains can help a lot here. In fact, I think that in many ways, but over time, blockchain will become the foundation of supply chains. You think about all the challenges that we are having right now getting medical equipment, and the challenges of hoarding, and so on. And we have got this ragtag dismembered subset of supply chains to the world where you got trains and boats and planes and trucks and bills of lading. And you know escrow agents and intermediaries and various kinds of systems and borders and immigration people and tax authorities. A lot of this is moving around with EDI (Electronic data interchange) - these **traditional primitive supply chain technologies with traditional ERP (Enterprise resource planning) and with paper and faxes and phones.**

Imagine if we had a shared network state for supply chains, - you know a real-time view of the whole asset chain of digital assets, as they flow through all of this, and digital assets representing physical assets of course. Then we can have

- a single version of the truth
- micropayments
- real-time supply chain knowledge
- transparency

No one is going to buy three years of toilet paper if they know that there is a supply chain that is going to deliver toilet paper tomorrow. This is basically an enormous opportunity.

Health Data

If you think about data today, this is obviously a very big problem. We are strong advocates of the notion of a self-sovereign health record system as a subset of a self-sovereign identity system, **and I believe that we can have our cake and eat it too.**

We can have all the benefits of:

1. **A self-sovereign identity** which are virtual data that you have generated as you go throughout life and that represents **your identity. That can be available to you to plan your life** which it is not right now. Instead it is captured by these large digital conglomerates and others that that use and exploit that data.

Smart Contracts to manage your private data.

So, imagine a scenario whereby we have a **self- sovereign identity healthcare record** that is sweeping up all data from your digital devices from various tests and measurements which are taken. They could include stuff like your real time heart rate, your temperature, and so on.

By law, governments could mandate in a crisis that citizens make anonymised data about clinical information (like their body temperature, location or wherever) available for adequate tracking. Predicted analyses of citizens data can instruct their digital identity to provide pertinent health information available to any registered clinician, should they need it. For example, hospitalised citizens may decide to withhold some information such as a fracture from an accident a couple of years ago, or a psychiatric problem, or something, but a smart contract managing their identity could release all the information if it would help with their treatment.

2. Secondly, we could **monetise the data** with appropriate assurances:

Data incentive systems.

We could have incentive **systems that could reward us for making our private data available to appropriate clinicians and even government planners,** even with identities attached. If we felt that that was appropriate lots of us would be happy to reveal our medical information about (say, our body temperature, or a dry cough for that matter, or a positive test for a coronavirus) to authorities to help manage the problem in our communities. But we could also have all kinds of other intrinsic blockchain-based incentive systems, and that is a big topic we have explored. All of these data would represent the population and not some weird partial sample which could be misleading. Never before in history of clinician's epidemiologist **authorities have had such extraordinary access to such a wealth of data.**

Using a next generation of data analytics and AI they could

- understand possible trajectories of a virus
- take steps to crush it in the egg, just like never before.

Individuals recovering from a virus develop a verifiable immunity. They could receive what MIT Sandy Pentland calls a **health certification to attach** to their digital identity to prove that they are safe to work publicly again. This is the old age-old conflict between the needs and rights of an individual, and the needs and the rights to society.

Many blockchain applications enter all kinds of opportunities for incentives to change the behaviour of billions of people through incentive systems that encourage **green behaviour** (e.g. **Tokyo tokenised carbon credits** or a company called CarbonX).

We could have a **rapid response system** for medical professionals and frontline professionals. The heroes, of course, are the heroes right now, and but hospitals cannot onboard them fast enough. There is a lack of talent, not the sense that there is a lack of talent per se, but just an inability to find them. We could build a whole new system streamlining coordination for talent among different geographies having certification for medical personnel helping us deal with all the border challenges, also to include the convoluted criteria of redundancies in the certification process. **Blockchain is about verification, accuracy, and provenance,** and so on, and finally a really big opportunity for us, we have to do with.

3. Thirdly, our data could be **secure** on blockchain systems**.** Right now, your identity is out there running on all these centralised servers which are hackable.
4. Forth, we could **protect our privacy.** People say to me "privacy's dead - get over it if you got nothing to hide". **I** think this is stupidity: **"Privacy is the foundation"** of freedom, and all this data represents our identity, so we need to get it back.

Sustaining the economy

The impact of this thing [the global health crises and COVID-19] is unfathomable economically. Two weeks ago, the unemployment rate in Canada was 5%, today it is almost 20%, and there are entire industries that are affected.

I am sure you could argue it is conjectural and it is all going to come back, but a lot of them are not. Consider personal travel, entertainment, anybody planning a cruise and even for business travel. Look, there is going to be PTSD (Post-traumatic stress disorder) for a long time. That is going to prevent us from wanting to rush off to some other continent for that meeting. In Canada, I think the oil and gas industry is finished, - the whole base of the Canadian economy for the last part of our history. There will be all these **big structural changes.** And you **combine that with all this other new stuff from technology,** as autonomous vehicles affecting the main job tasks of the truck drivers in 48 of 50 states the United States. I think that is not a job gone in 50 years, and it is gone in a decade.

A new social contract

We are going to need a new social contract and ideas like a guaranteed universal basic income are ideas whose time has come, maybe. We need to take a whole bunch of steps to build a new kind of innovation economy. And how we could help fund entrepreneurship and a really big one. We need to move to **digital cash,** and not just community-based cash like Bitcoin or corporate-based cash like Libra. Every country should have one, and I think Mark

Carney [Governor of the Bank of England from 2013 to 2020] is right when he mused that they **should all be rolled up to a global synthetic hegemonic cryptocurrency.**

Insurance has been mishandled at many levels, and there are all kinds of ways to protect people and businesses from catastrophic risks. We have all these decentralise models of governance and organisation problem solving that can reduce the costs in healthcare delivery and help NGOs and others that **raise funds. Individual donors contribute** money and other resources to fight against the COVID-19, and so on, and not to mention all the big changes to the financial system reducing counterparty risk that brought down the capitalism (financial crises) in 2008. So, **there is a whole cluster of opportunities** that have to do with the financial system.

An Emergency Task Force on Medical Data

Dozens of actual companies are working on this, but **governments need to wake up to blockchain.** It is not about or machine learning or the Internet of Things or any of the rest of that. These are great wonderful technologies, but this is **all about the data** itself, about creating a **secure transactional platform** for our economy.

Every national government needs to create **an emergency Task Force on medical data** to start planning and implementing blockchain initiatives. They can **stimulate the development of technology firms** working on the solutions that we talked about through all kinds of ways:

1. **governments can be a model user of the technology, where governments** can focus on the supply side for market data, not just the demand side.
2. governments are the world's largest supply chains they should be using this technology for their own supply chains piloting cases

it means

3. **passing legislation** to mobilise stakeholders around
4. creating self-**sovereign** identities and citizen-owned health records

they should

5. pilot blockchain and incentive systems for motivating people and having them behave responsibly
6. partner with medical professional associations and other players to implement blockchain-based credential systems
7. central banks should move quickly and swiftly to create **Fiat digital** currencies in their country, and the IMF should take a leadership role in rolling these **up to a global synthetic hegemonic cryptocurrency.**

Useful sources.

The Blockchain Research Institute has published several projects on blockchain-based identity systems. These projects dive into the concept of how blockchain technology supports user-centric and self-sovereign identity solutions that enable users to own securely, store, share, and potentially monetise the data they generate as they go about their daily lives.

In the “Blockchain Revolution in Education and Lifelong Learning” by Don Tapscott and Alex Kaplan, this project explores how blockchain is transforming education with an emphasis on lifelong learning and the reskilling of the workforce. It covers not just traditional educational institutions but also corporate training and development, where innovators are using blockchain to establish student identity, protect privacy, finance coursework, measure progress, and record badges of achievement and skills mastery.

In Blockchain Identity Services: Technical Benchmark Of Existing Blockchain-Based Identity Systems by COALA’s Greg McMullin, Primavera de Filippi, and Constance Choi, the authors explore the specific technical elements which make blockchain-based identity applications feasible, such as public-key cryptography, hashing functions, zero-knowledge proofs, and homomorphic encryption, as well as the benchmarks used to evaluate one solution from another, including governance, system architecture, and user experience.

A third project, Accessing Patient Health Records via Blockchain: University Health Network’s Patient Control and Consent Pilot with IBM by David Carter, explores how Canada’s largest hospital network leverages blockchain technology to improve patients’ rights and control over their health records. It provides a blueprint for how patients and data custodians can make private health records more transparent, portable, and under the rightful control of the patient.

2.2. Taavi Rõivas, Estonian MP and Former Prime Minister, Estonian Parliament

Feature: Taavi Rõivas explains how Estonia is built as a digital nation since it became independent in the early 1990s, including all the details of the country's institutions and information systems. Blockchain was adopted before that it was called blockchain, but then called 'hash linked time stamping', and since 2008 e-health and the healthcare registry has operated on the blockchain (alongside other registries, such as those related to property, business and succession registry). Safety is important and blockchain cannot, or should not, be used if cannot make the data fully private.

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence giving: Taavi Rõivas

First, a very short introduction about Estonia. Estonia became independent again in the early 90s, in 1991, and why is that important? **We needed to build a country, including all the details of a country's institutions and information systems. We needed to build it from scratch**, so basically, we did not have any legacy and we needed to introduce the best technology that was around. And of course, the 90s was also the time when internet became a thing and thus it was very logical to build a very digital country from the beginning.

The most important cornerstone for us, and difference from many other countries, is that **already from the beginning of this century we started using digital identity and digital**

signatures. This means basically that every single Estonian has to have a digital ID. You can have a passport, but this is optional, but the digital ID every Estonian must-have.

I know that in 2020 it's not so much of a rocket science anymore and many countries actually have their own versions of digital identity, but perhaps it's interesting to know that **more than half of all the Digital Signatures in the world are still today given by Estonians** and if you wonder how many of us are around there it's only like 1.3 million. So, either the rest of the world is not signing enough, or we are just signing like crazy, so go figure which one is correct. Taking everything digital by default has given us the opportunity to not only save paper, and this is also relatively useful, but of course it has **given us the chance to save a lot of time and make things a lot more efficient**.

Let me just give you a couple of examples:

- Tax: When an Estonian declares taxes it takes you usually less than 2 minutes because all the companies have already declared the income of all the people so basically what is happening in the background is that the system knows already how much money each and every citizen made and, you as a citizen just need to go and have a look if everything is there. If you, let us say, made some income from another country and this is not linked to the Estonian system, or that resilient tax authority doesn't already know about it, you just need to add it manually. But you know, other than that, you basically go through with five clicks and confirm that everything is correct, and that is all you need to declare your income. The same applies to the most important thing citizens, governments and businesses are part of.
- Health: Ever since 2008 all the medical data of each and every Estonian is in one central system. It is called e-health. It's, of course, digital and this means that if an Estonian living in Tallinn, which is the capital at my hometown, is taken to hospital in Tartu, which is the second biggest university town 200 kilometres south, the doctors then can get your full medical record. This helps a lot because they know a lot about you, and often do not need to rerun all the tests and so forth. This is with your consent of course, but or if you are unconscious, then the consent is basically not taken

Blockchain has helped us to safeguard many of these important information systems in this way that we keep the data records intact. If you build any digital information system - especially in a government context and public system - you need to make sure that the data is not attacked in any way. Thus, it is extremely important that the data safety and integrity is a place and **blockchain is something that we have been using from before that it was called "blockchain".** In 2008 obviously it was not called "blockchain". Back then it was called 'hash linked time stamping' but it is very close to the today technology that we are calling blockchain, and that is how we keep all the registers. A few of those where we are using blockchain to safeguard the data, including healthcare registry, property registry, business registry and succession registry.

About data privacy: It is a very important question because **blockchain, as we know, cannot or should not be used if you store data which you cannot make fully private**. So basically, we do not store all the data in blockchain, but only certain ‘hashes’ sufficient to make sure that the data is not meddled with, but it doesn't give out any of the data itself. These things are especially important when we are talking about health, for example.

2.3. Angel Martín, Spanish representative in the Policy and Technical Groups, European Blockchain Partnership, Ministry of Economic Affairs & Digital Transformation (Spain)

Feature: Angel Martin explains how 'digital credentials' in a self-sovereign identity blockchain model under the control of the individual, means increased privacy, improved interoperability without a central database, and can operate with a cross-border dimension. Also, there are many applications for the health care sector for tracing, tracking, and controlling vaccinations, prescriptions, medical records, health insurance, drugs, and infections on people.

Angel Martin
Spanish representative in the Policy and Technical Groups,
European Blockchain Partnership,
Ministry of Economic Affairs & Digital Transformation

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence giving: Angel Martin

Good afternoon, Ladies and Gentlemen. I appreciate the opportunity to address this meeting, and I am honoured to speak to this institution.

I work at Spain's General Secretariat for the Digital Administration, which is part of the new Ministry of Economic Affairs and Digital Transformation and is the public organisation in charge of digital transformation for the central government. In short, we design and deploy digital services for citizens and public administrations.

We are participating in national and international forums related to blockchain, such as the European Blockchain Partnership (EBP) that is collaborating towards building the European

Blockchain Services Infrastructure (EBSI) spanning representative in both the policy route and the technical group to coordinate the EBSI deployment. At the start of 2019, EBP started exploring out three Blockchain use-cases: **(1) Digital Identity, (2) Education Credentials (Diplomas) and (3) Notarisation of Document.**

All of these use cases met **three consistent criteria: (1) having something to do with a public service delivered by a Public Administration; (2) possessing a cross-border dimension; and (3) being a use case in which blockchain technology offered added value**.

In February 2020, the first testing version of the EBSI network applied to those use cases was launched.

Evidence has emerged that the self-sovereign identity use-case is not an ordinary use case and that it was not at the same level as the others since it is necessary to know beyond any shadow of a doubt who the individual associated with any credential is. Moreover, all other 'digital credentials' are an 'identity attribute' of an individual or use case.

Evidence has emerged that the Self-Sovereign Identity use case is not an ordinary use case and that it was not at the same level as the others**. Identity is the foundation upon which all other use cases are based**. Moreover, all other 'digital credentials' are an 'identity attribute' of an individual or use case.

This use case, in combination with the eIDAS regulation, **allows a cross-border identification** based on blockchain where each country may use their national identification means in an easy way with high level of assurance.

The self-sovereign identity model results in enhanced DATA security. I will mention only four points:

1. Personal data is held by the individual citizen and not information silos. The consequence is a population that is more protected from traceability or user profiling analysis as well as from manipulation and the Big Brother effect. The system does not prevent service providers from accessing the personal data of their users and customers, but it does establish **a way for the individual to (i) give or (ii) withhold his/her consent linked to a specific purpose as well, as a way to withdraw not consent. This facilitates both actions and thus restoring control to the individual**

2. **Data on blockchains are more secure against computer attacks or hacking because personal data is not housed in a single system but in many**. In addition, if one of the nodes is attacked the others immediately detect change. Facilitating early attack detection, one of the hallmarks of an enhanced security system. That is possible because of the consensus algorithm to reach an agreement between the parties about the information to be registered in the ledger. The cryptographic elements are on blockchain also reinforce the security of the information. Moreover,

the elliptic curve type of the algorithm using blockchain is more robust than traditional cryptographic algorithms.

The use of self-sovereign identity generates enhanced security against computer attacks (hacking) as:

- Information is not housed in a single system but in many.
- If one of the nodes is attacked, the others immediately detect the change, thus facilitating early detection of attacks, which is one of the hallmarks of an enhanced security system.
- The elliptic curve-type of the algorithm used in blockchain is more robust than traditional cryptographic algorithms.

3. **Blockchains enhance transparency and minimise institutional corruption.** This effect is derived from the greater difficulty applied to manipulate or alter information. For example, in Spain there is a blockchain tender project that guarantees that no-one can access the content of the offers before submitting them. In short, each and every applicant presents the hash of their offer before the deadline. After the deadline, everyone submits their offer, which must exactly match the hash presented before that time. In addition, the transparency of this process **has a leverage effect on the market.**

4. **Participatory and legislative processes become more secure and transparent** with blockchain technology.

Regarding the question of whether self-sovereign **identity on blockchains helps in the fight against COVID-19 and other global pandemics**. There are **many applications of blockchain technology in the self-sovereign identity model that are appearing in the health sector,** such as:

- registering vaccinations certificates
- medical prescriptions
- the possession and control of medical records by the individual
- health insurance cards on the blockchain
- control of pharmaceuticals
- the ratio of the infected people is written into a blockchain network (for study and analysis of the expansion of the infectious disease)

All these examples are 'digital credentials' that **in a self-sovereign** identity model are under the control of the individual, which means **increased privacy, improved interoperability without a central database, and could work in a cross-border dimension**.

Finally, some of the main ingredients for success with this technology are **training** and **education.** Also, **collaboration** and agreement are needed between all parties, and finally, **awareness** that blockchain will not substitute all the current centralises models that we are using now, but we have to be able to recognise those uses that are best suited for blockchain technology.

2.4. Marta Piekarska-Geater, Director of Ecosystem, Hyperledger (UK)

Feature: Marta Piekarska-Geater argues that there is space and need for a decentralised autonomous self-sovereign identity system. That is where data belongs to the user, or to the humans, or to the devices, rather than centrally controlled Authority. *Blockchain provides this solution, and Hyperledger (Linux Foundation project) provides this open-source. There is evidence from the health sector (e.g. on HIV use cases) that such a special system creates incentives for data sharing, as it provides safe control to people on how their data are used, and it allows the health sector to protect electronic records of patients into cases of sensitive diseases. Finally, it allows (in principle) users to trace the interactions with people diagnosed with a disease that is contagious, in a privacy-preserving and secure way.*

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence Giving: Marta Piekarska-Geater

Hyperledger is a Linux Foundation project. Linux Foundation was created over 20 years ago to promote and provide governance and infrastructure for open source projects. It started with **core Linux and today it grew to over 120 different projects** in every major industry. We have projects like (i) Cloud Native Computing and (ii) LF Energy, a project that recently started to see how open-source technologies can with the use of **blockchain support fighting climate change** and provide **sustainable energy** sources, (iii) and we do all other sorts of projects.

We want to create the largest shared technology investment in history. We believe that together **we can create something much stronger than individually**. In this spirit three-four years ago we created Hyperledger. It was created by 30 different enterprises that came to the Linux Foundation and said, what do you want to do about this whole Blockchain space. How can the Distributed Ledger Technology (DLT) that underlies Bitcoin contribute to enterprises on a day to day basis? We have grown over the years to a very big project, one of the fastest-growing projects within the Linux Foundation. Hyperledger has become an open-source collaborative effort to advance cross-industry blockchain technologies. It is hosted by the Linux Foundation and it really stands over and across all sort of domains.

We have a very modular approach to software projects, - we like to call it the 'greenhouse' because **anybody can come with a seed of their idea and plant it into the community.** If the community wants to feed the plant and help it grow, then it will grow to something beautiful. We have 14 different projects. They are grouped into DLTs, tools, libraries and domain-specific projects. In the light of today's topic Hyperledger Indy, Aries and Ursa are the three that are worth highlighting. These allow to build secure and privacy preserving identities rooted on a blockchain.

We do not believe that blockchain will solve all the problems, but we do believe that **there is a space and need for decentralised autonomous systems and self-sovereign identity**. That is system in which **data belongs to the user -- be it humans or devices -- rather than to a centrally controlled Authority.**

Indy is an independent identity within Hyperledger. It is a special-purpose build blockchain. It uses a Byzantine Consensus which reduces the cost and improves the throughput.

Many projects are just being built out and are not well tested. I would like to focus on things already being used in response to the perils to the world that we have today.

The first one is a **special system that allows you to protect electronic records of patients into cases of sensitive diseases,** like HIV. Using this solution out of almost 9,000 patients almost 100 per cent accepted to be tested, 99% come and 86% agreed to register. This is unheard of acceptance of HIV testing, especially in Africa. Here you can think of the same thing of what happens when we need to test people for COVID-19.

In addition, a private kit was developed at MIT and is an app that allows you **to trace the interactions with people,** but if you get diagnosed with a disease that is contagious, this also allows you to do it in a privacy-preserving and secure way. The app monitors at the traces rather than precise location. Finally, company called Ledger Domain built a consortium for the pharmaceutical supply chain.

Why I am talking about it? Because I want to consider what happens tomorrow when we have a vaccine. To be able to **prevent fraud** and to make sure that the COVID-19 drugs, and any other pandemic drugs, are **raising value** and **costs controlled**.

Trust in key institutions has been steadily declining over the past two decades. Economic crises, fake news and global pandemics bring a need for transparency, security, and provability of information.

Business today is no longer based on personal interactions. We are being asked to put faith in email addresses and phone calls. In a globally connected world, business records need to be immutable, auditable, thus trusted. Distributed Ledger Technology brings the promise of changing the way we interact, make businesses, and receive information. Everyone in the network is now able to verify claims others are making.

In the times of global pandemics, the opportunity for Permissioned Public and Private networks is massive - from proximity tracking to verifiable credentials. Blockchain in its permission-less incarnation cannot provide the control and verifiability of what gets submitted to it. In permissioned systems, who can own a node is limited by defined rules. Such setting brings all the advantages of DLTs - immutability, auditability, transparency, and security - while ensuring that the data can be trusted. No more of "garbage in, garbage forever" situation.

DLTs can immediately help improve the current situation, by creating trusted credential systems, tracking of movement and exposure, and infection rates. What is even more important, this technology will also be crucial in the post-pandemic world—securing the pharma supply chain to prevent distribution of fraudulent medication, restoring the equilibrium in the global economy, and creating better rapid response systems.

It is amazing to see how technology can bring hope for a better world.

2.5. Andrew Tobin, Managing Director EMEA, Evernym Inc (UK)

Feature: Andrew Tobin argues how the Covid-19 pandemic is the catalyst for massive acceleration to solve the digital trust problem, i.e. trust at a distance. He advocates for digital versions of the credentials which we can all have globally. They need to be interoperable and verifiable anywhere. He calls them "verifiable digital credentials". It is not just about identity. Credentials could be anything that conveyor certification and entitlements or achievement, and they all need to work online as well. They are needed for all trusted systems and to increase mobility of health workers and others.

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence giving: Andrew Tobin

I work for a company called Evernym and we are a US-based tech company. We are the originators of much of the technology of Hyperledger and others, in this new world or the new generation of digital identity and Trust, being called self-sovereign identity or decentralised identity.

Let us look quickly at the implications of COVID-19. First, we think that **there is going to be a massive increase in the need for trust at a distance,** so for example, doctors will be doing consultations remotely. How do you know it is a doctor? How does a doctor know it is the right patient? You can see a very **rapid increase and the need to prove who you are digitally,** quickly, and easily. We already have that need, but COVID-19 and all the implications of remote working and low [physical] contact, really catalyse that increase.

Also, it is not going to be good enough to have something that works in one country or in the EU. You are going to need something that works globally, is globally acceptable and which is interoperable globally. Something that does not result in lots of unintended identity correlation and does not compromise security and (as Geoffrey Goodell argues).

We need digital versions of the credentials we all have **globally.** They need to be **interoperable and verifiable anywhere** and we call them **verifiable digital credentials.** It is not just about identity. **Credentials could be anything that conveyor certification and entitlements or achievement,** and they all need to work online as well.

So, let me give you some examples of what is happening in the world tomorrow. To give you some projects, here is one that is directly pertinent.

Trusted digital identity and single sign-on for medical staff solving the problem of a doctor, is taking a day or more to get authorised. To work in a hospital that medical staff just arrived at to do a specific job, or to respond to an emergency, usually take a day or more, but we can get them onboarded down in 15-20 seconds. Just at the end of last year we ran a successful pilot with the NHS and NHS X and UK company called True (the CEO of which was meant to be speaking here, but he is an infectious diseases consultant Northeast London which is why he can't be here at the moment).

It proved that by **issuing digital credentials** to doctors about their GMC certification license, to practice their medical degree, and so on, they could onboard into a new hospital in seconds and not days. And once they have done that, they could also use their digital credentials to log in to hospital systems without needing usernames or passwords either. There is work ongoing at the moment with the NHS as you can imagine. I cannot speak any more about that, this would be for the NHS to do, but I think you can see the potential there.

Other things happening in the world of digital credentials there is a GLOBAL COVID-19 CREDENTIALS INITIATIVE that is being kicked off. The first call had a hundred and fifty people from sixty organisations around the world looking at how can you take the new technology of **digitally verifiable credentials and use them** globally for specifically COVID-19 responses. For example, have you received a test, what were the test results? Have you had the disease, what the results? Are you okay to fly? etc. Again, the focus is on global **interoperability whilst enhancing the privacy and security of the individual and not creating a huge global centralised database that tracks everything you do.** These are the building blocks.

Evernym is very proud to have contributed a lot to the open standards and this is a real focus here. You cannot go down that a route that is proprietary to a single organisation. You have to have something that is based on open standards and open source. We use **a global utility**

for storing public keys of credential issuers, and the one we use is sovereign identity which is a running blockchain. If you use Hyperledger, then the four component you need is 1) the ability to actually issue and 2) verify digital credentials, 3) unique platforms to do that, and that 4) this is an open competitive environment. We have one [a platform] out there already, that is being used. Other organisations that do that as well are built on the same open-source technology.

So, in summary, what is special and what is new?

- **Anyone can issue a digital credential** about anything to anyone else just like you can issue a piece of paper, pass a ball, a letter, whatever it may be.
- **Anyone in the world can verify the origin, authenticity, and** integrity of any digital credential, and
- the same capability can be used to secure **authentication and communication**
- **Avery interaction is private secure and encrypted** by default, and
- this can be achieved **without needing a huge privacy busting central database** and
- **without all parties need to have meetings or have expensive technical integrations** with each other.

This is why digital identity does not work very well at the moment.

Enabling "trust at a distance" is vital as the economy becomes more digitised. The Covid-19 pandemic is the catalyst for massive acceleration to solve the digital trust problem.

Vast friction has been introduced into current digital processes simply to confirm who (or what) is at the other end of a connection. This is extremely costly and inefficient. Worse still, every organisation does things differently, meaning that trust is stuck in silos and does not work at internet scale.

To fix this problem, experts from around the world have created new global standards and open source technology for issuing, holding, and verifying digital credentials. Such credentials could be a passport, doctor qualifications, driving license, student ID, a plane ticket, or an inoculation certificate. Literally anything that can be printed on a piece of paper or plastic can be made into a digital credential.

This means that anyone, anywhere, can issue digital credentials about anything, directly to people (or organisations), who carry them and manage their use, just like they do with their paper and plastic credentials today.

What is more, these credentials can be presented to any organisation anywhere and immediately verified as authentic. The verifier (e.g. a border guard, hospital administrator, airport check-in attendant) can check who issued the credential, that the data hasn't been tampered with, that it was issued only to the person presenting it, and that it hasn't been revoked. All in 5-10 seconds, and without having to "phone home" to the credential issuer.

This capability does not require a vast central "all-seeing" database run by a single company or government. The highest levels of privacy and security are built in to prevent people's actions being correlated across different interactions. Additionally, it is not reliant on any single vendor as it is based on open standards and open-source code.

Taken as a whole, this new capability is being termed "Trust Over IP". Evernym is a leading developer of many of the underlying technologies and is currently working with the NHS on a Digital Staff Passport that utilises these open standards.

2.6. Geoffrey Goodell, Senior Research Associate, UCL Centre for Blockchain Technologies (UK)

Feature: Geoffrey Goodell explains the uses of blockchain to benefit national security, including tracing and tracking the provenance of everyday physical products, intangible goods (e.g. software), including information of the marketplace. He also challenges alternative blockchain designs and argues how credentials of people must not be linked (e.g. to one Master Root Identity). Instead, he advocates for the use of systems allowing for multiple identities to ensure the people's control over their data, and better security. For blockchain designs, he considers the balance of power between the individual versus the state or the big tech companies.

Geoffrey Goodell
Senior Research Associate Financial Computing Analytics
University College London

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence giving: Geoffrey Goodell

First of all, there are many potential ways to use blockchain & DLT to benefit national security. For example, we can use distributed ledgers to trace the provenance of the component parts of the many products we use each day, including the food we eat and the devices we use. In this manner, the product components can be tracked and traced, and we can even use this information in marketplaces, for the purpose of levying tariffs, recalling products, informing consumers, and monitoring business practices.

We can use DLT track other things as well beyond physical goods. Software updates, targeted adverts, campaign finance -- all of which are relevant to national security. And in each case, the solution can be designed to be human-oriented security: empowering individuals and businesses to make informed decisions about their security, and thus benefiting society as a whole.

We can use distributed ledgers to

- **Trace the provenance** of the component parts of the many products that we use every day, including the food we eat and the devices we use. The product components can be tracked and traced.
- We can even use this information in marketplaces for the purpose of **levying tariffs, recalling products, informing consumers, and monitoring business practices**.
- We can also use Distributed Ledger Technology (DLT) to **track other things as well, beyond physical** goods, as
    a. software updates
    b. targeted adverts
    c. campaign
    d. finance

All the above are relevant to national security.

In each case the solution can be designed to achieve human-oriented security, which is to say it can be designed to empower individuals and businesses to make informed decisions about their security, thus benefiting society as a whole.

But we must be careful with the subject of tracking humans themselves. The digital identity of human beings is an area wherein we need to think very carefully about human rights before we design and implement systems, because the systems will have a profound effect on **the power relationships that individuals have with businesses, institutions** and governments.

Many digital identity systems work by giving every person an identity number and expecting **that these persons will use that number again and again in different contexts, thus creating a permanent record of all of their activities.**

But the people are not the enemy, and if we believe that the people are the enemy, then we have lost the plot.

We must first ask, 'cui bono?' -- who benefits -- from the design and implementation of digital identity systems. In general, the beneficiaries are large corporations or state actors who believe that they can reduce their risk by knowing how individuals behave, or, increasingly, by controlling and constraining how individuals behave through record-keeping, incentives, and punishments.
Recently there has been a burgeoning **fascination with self-sovereign identity systems** in

which individuals are able to use different identifiers and different contexts. Self -sovereign identity approach might seem to solve the problem of individuals being assigned numbers; however, as it turns out, the expectations (of the effect of self-sovereign identity systems) do not always square with the reality, and we must not fall prey to their siren song.

Nearly all of these so-called self-sovereign identity **systems rely upon a 'master' or 'root' Identity, or some other mechanism, to ensure that all the credentials that a person might create are linked to a single unitary avatar.**

Some of these systems such as ShoCard and Everest **accomplish this explicitly using biometrics to bind all of the credentials that an individual might create to a root identity that they cannot change**, while others such as uPort and Chainspace accomplish it implicitly**, by providing a cryptographic means of proving that two credentials are linked, thus ensuring that relying parties would ask for this link**.

Unfortunately, it turns out that if a link between two attributes or credentials can be proven, then that link can be forcibly discovered. It is the requirement **that each person can have only one root Identity that influences and constrains** how individuals can behave.

If we want to preserve the freedoms that individuals enjoy in the real world without changing the balance of power, then we need to ensure that they have the means to create multiple unlikable identities. I call this **the inalienable right to alienable identities.**

For the avoidance of doubt, it is technically possible to design digital credential systems to allow everyone to have multiple un-linkable identities, but in the quest for **high assurance, such designs have mostly been ignored.** But more assurance is not always better. In fact, the greater the assurance needed for a particular use case for a digital identity system, the narrower and more limited that use case must be.

By and large, **digital identity systems represent a shift in power from the vulnerable who are punished for unclean records, to the powerful who will be able to exploit them.** There must not be one ID system to rule them all, and we will not succeed as a society if we force people to submit to having all their actions be discoverable and linkable. **Such a system would not enforce national security; in fact, it would introduce insecurity for those who need security the most.**

2.7. Jonathan Levi, Founder, HACERA & Unbounded Network, MiPasa (USA)

Feature: Jonathan Levi explains how the success of Blockchain implementation to various use-cases, including for COVID-19 and related trusted tools analytics and applications, requires a trusted ecosystem coordinator for data capture (e.g. WHO, ECDE), distributed data storage, crowding in analysts (university research people and institutions), top cloud providers and Big Techs working together. Hackathons have proven useful as well.

APPG Blockchain Webinar 8 April 2020

Below is a creative copy-edited version of the transcript from the evidence giving, created for presentation purposes. We take responsibility if any errors have occurred.

Evidence giving: Jonathan Levi

We basically started **working on a data platform** which should serve as a basis for COVID-19 and related trusted tools analytics and applications. Many people here talked before about the limitations of blockchain technology, and I think it is really important to understand that the virtual is not going to solve everything, but it can solve a few things. I have been working on blockchain for many years I was working on Bitcoin before Ethereum was even launched.

What we wanted to **collect a lot of publicly available data at Phase one** [of the COVID-19 crises] and to try to look at official data sets that are published by the WHO [World Health Organization], ECDC [European Centre for Disease Prevention and Control] and different countries, as well as local authorities. We just wanted to focus on three things:

1. Firstly, to make sure that **the integrity is there**, meaning that when I refer to a file, it is very clear that I refer to the latest version the WHO public record
2. Secondly, to assure there some **security in terms of nobody is tampering with the data** on the fly or in storage.
3. And the third thing, we didn't want to create another honeypot where we store everything in one location and actually take away privacy by allowing different data that don't have Personally Identifiable Information (PII) on their own to basically triangulate. Other people can take advantage of that, and people mentioned privacy a few times here.

I think that the **biggest problem that we have is privacy and especially in a crisis mode in an emergency government or in any jurisdiction, people forget this one thing**.

Once these data are out about my age, about my past history, about any sensitivities whatever they are, **you cannot opt-out of these databases.** It just out forever. This is why I think that we need to be very careful. The main goal here is actually to provide government-institutions involved with making decisions, **to start making *informed* decisions, and that also includes businesses regulator**s.

There are so many people that we need to get data from, and it is just scattered everywhere. You can somehow gather it and we saw **a lot of hackathons working really hard and spend a lot of time to try to build some models and tools**. Some of them have really beautiful charts but they break it after two dates because the API is not there.

Building ecosystems

We want people to submit data to us because we analyse it, and we have a team of lots of university research people and institutions that would like to help and contribute. So, we have data from one end and analysis from another, and **the idea is to take this opportunity where people are actually listening and working together**.

We get like top cloud providers and Big Techs all working together, and basically what we do, **is to engineer the data in a way that does not change it.** We prepare the data so that people can consume it in an easy way. **We do not write all the analytic models, but we integrate with external analytics. Blockchain is not about AI and machine learning**.

I would still like to have **a single version of the truth**, and that should be the source for all these heuristics and all this analysis, that analysts are going to run. We provide people with something that we call **an API freeze** so even if there are structural changes, we still provide some data.

It is very easy to go to World Bank [and other official providers as national statistics, WHO and ECDC] to get official data sets, and people know that if they go through our system (i), it has not been tampered with, (ii) they can easily consume it, and (iii) it will stay like that for a while. So many people are helping everywhere around the stack, and we are looking for more data and more people that would like the data and anything in between.

Contact details

APPG Blockchain Secretariat

Big Innovation Centre
62 Wilson Street
London EC2A 2BU
United Kingdom

info@biginnovationcentre.com
www.biginnovationcentre.com

www.biginnovationcentre.com