Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law
&
Security Review

E-residency and blockchain

Clare Sullivan [a,*], *Eric Burger* [b]

[a] *Law Center, Georgetown University, Washington, DC, USA*
[b] *Department of Computer Science, Georgetown University, Washington, DC, USA*

Keywords:
E-Residency
Blockchain
KYC
Data protection
Digital identity
Right to identity

ABSTRACT

In December 2014, Estonia became the first nation to open its digital borders to enable anyone, anywhere in the world to apply to become an e-Resident. Estonian e-Residency is essentially a commercial initiative. The e-ID issued to Estonian e-Residents enables commercial activities with the public and private sectors. It does not provide citizenship in its traditional sense, and the e-ID provided to e-Residents is not a travel document. However, in many ways it is an international 'passport' to the virtual world. E-Residency is a profound change and the recent announcement that the Estonian government is now partnering with Bitnation to offer a public notary service to Estonian e-Residents based on blockchain technology is of significance. The application of blockchain to e-Residency has the potential to fundamentally change the way identity information is controlled and authenticated. This paper examines the legal, policy, and technical implications of this development.

1. Introduction

> *"We are doing this as a start-up. We don't know the full implications. Of course, we are hoping that it could be disruptive."*[1]

In December 2014, Estonia started issuing e-ID cards to e-Residents and became the first nation to open its digital borders to foreigners, through its e-Residency initiative. For the first time, a nation has enabled anyone anywhere in the world to have an international digital commercial life using a sovereign government-backed identity credential. E-Residency is an evolution of digital identity programs, and the Estonian program is currently the most advanced government-sponsored, consumer digital identity program in the world.

E-Residents are able to remotely access and use a range of Estonian e-government and private sector services. The e-ID issued to Estonian e-Residents enables commercial activities including business and company registration, opening of bank accounts and funds transfers, buying and selling of real estate and other property, and trade of goods and services.[2] Digital trust services (e-trust) enable documents to be executed, and

* *Corresponding author.* Law Center, Department of Computer Science, Georgetown University, Washington, DC.
E-mail address: cls268@georgetown.edu (C. Sullivan).

http://dx.doi.org/10.1016/j.clsr.2017.03.016

[1] Interview with Siim Sikkut, ICT Advisor, Government of Estonia, "E-stonia – A Startup Country", Back Light, June 15, 2015 at https://www.youtube.com/watch?v=9bYpk75JnZU&ebc=ANyPxKrsZWcc0C96ssbtS4rY-mHWwtx0k14wmTIcFI5OMfZvG-Ce9bSH2kJmQTzK86OSgEIYGSr388b9iB2twRWAt1I2sk6XNg.

[2] Since Estonia joined the euro zone on January 1, 2011, Estonia has brought its anti-money laundering regime into compliance with international standards. The Financial Institutions and e-Money Institutions Act (now the Payment Institutions and e-Money Institutions Act) was enacted by Estonia in 2010 and the Estonian Penal Code provides for asset seizure and forfeiture, and contains provisions dealing with money laundering. See Penal Code Passed 06.06.2001 RT I 2001, 61, 364.Entry into force 01.09.2002 at https://www

notaries avoided, with an electronic signature. There are limits to e-Residency, however. It is not residency or citizenship in its traditional sense and it does not provide a right to physically enter Estonia or the European Union (EU). E-Residents also do not have access to the full suite of the services available to Estonian citizens and permanent residents. E-Residency is primarily a means for expanding the commercial base and economy of Estonia,[3] but it is important because it entails the issue of a government-authenticated digital identity.

The stated goal of the government of Estonia is to have 10 million e-Residents by 2025.[4] For comparison, the entire population of Estonia is under 1.3 million.[5] Since the launch of the Estonian program, the number of e-Residents has steadily increased, exceeding the Estonian government's estimates threefold.[6] As of February 2016, 8500 people from 135 countries have applied to be Estonian e-Residents, with 8000 ID cards being issued.[7] To date, 320 e-Residents have established a company and another 720 companies involve e-Residents as owners or board members, for example.[8] While most e-Residents were initially from neighboring countries, the new trend is from Asia, particularly from India.[9] In 2016, Estonia reportedly wants to target Singapore, India, and the US for its e-Residency services.[10]

New services were added to the e-Residency program in 2015 and more are planned for 2016. Many of these services go beyond doing business in Estonia. The smart ID card issued to an e-Resident enables use of digital authentication for a range of applications. The Estonian e-Residency team is working with private companies to provide universal authentication services, the most significant of which is the application of blockchain technology to authenticate identity and identity documents.[11] This development is especially significant because the Estonian government and its infrastructure support it.

The Estonian e-Residency program is very attractive to individuals who wish to participate in economic activity[12] and businesses[13] seeking to expand their economic base. Estonian e-Residency team product manager Ott Vatter says:

> *"it's the most efficient way of getting benefits like easy access to the EU market, e-banking services, and a streamlined digital administrative system. An entrepreneur doesn't need to be an e-Estonian to do most of these things, but it usually takes a lot of time, effort, money, and a physical presence to get all that going."*[14]

Other countries and regions are likely to follow Estonia's lead and will similarly open their digital borders. The Estonian e-Residency model is also likely to set the standard for Europe. Mutual recognition throughout the European Union is a key component of the Digital Single Market strategy adopted by the European Commission on 6 May 2015 that includes 16 initiatives to be delivered by the end of 2016.[15] Most importantly therefore, while the primary objective of the Estonian e-Residency initiative is to attract business and investment to Estonia, it facilitates broader access to Europe and the planned Digital Single Market.

There are indications of this development now. Estonia, Belgium, Portugal, Lithuania, and Finland mutually recognize their e-IDs. In December 2015, Estonia and Finland became the first countries in Europe to develop a joint data exchange platform based on Estonia's X-Road, the platform that is also used for Estonian e-Residency. This platform enables databases in Estonia and Finland to interface to make e-services accessible to Estonian and Finnish citizens and permanent residents.[16]

.riigiteataja.ee/en/eli/ee/Riigikogu/act/523122015005/consolide; and the Payment Institutions and e-Money Institutions Act) passed 17.12.2009 RT I 2010, 2, 3 entry into force 22.01.2010 at https://www.riigiteataja.ee/en/eli/511112013017/consolide.

[3] The Estonian government launched e-Residency to make Estonia bigger: to grow our digital economy and market with new customers, there-by sparking innovation and attracting new investments. In addition, e-Residency makes life and business easier and more efficient for everybody who already have a business or other relation to Estonia. See, Government of Estonia, "Estonian e-Residency First Anniversary", December 1, 2015 at https://www.youtube.com/watch?v=exyg1Eybcjw.

[4] Government of Estonia, "Estonian e-Residency First Anniversary", December 1, 2015 at https://www.youtube.com/watch?v=exyg1Eybcjw.

[5] *Estonia*, The World Factbook, Central Intelligence Agency, retrieved June 5, 2016.

[6] Ibid.

[7] Government of Estonia, "Estonian e-Residency ", February 2016 at https://docs.google.com/presentation/d/1hUHyYKWspu4k3K1OU9WCSSEk8D6jaZwjrsB1c7Ljick/edit?pref=2&pli=1#slide=id.gaf21f25ad_0_0.

[8] Ibid.

[9] Presentation by Kaspar Korjus, Estonia e-Residency, n 2 above.

[10] Michael Tegos, Estonia's e-residency program makes it easy for Singaporeans to do business in the EU, TechAsia Feb 4, 2016 https://www.techinasia.com/estonia-e-residency-singapore-entrepreneurship.

[11] Announced in December 2015. See n 4 above.

[12] According to the head of the Estonian e-Residency program, Kaspar Korjus, "there have been numerous requests for information from countries that suffer from lack of proper digital identification and therefore have limited access to digital services. These people see e-residency as the first service to allow them to enter into a modern digital society." according to Korjus. See, "E-residency – up against great expectations", January 13, 2015 at https://e-estonia.com/e-residency-up-against-great-expectations/.

[13] "On the other hand, you have all the service providers that consider the overhead of establishing a presence in every country in the world too big. E-residency would open up new markets without the need to sign a deal with all the different banks and merchants there. They would just need to recognize Estonia's e-residency and sign a deal with an Estonian bank that hosts e-residents," Korjus explains. See, "E-residency – up against great expectations", January 13, 2015 at https://e-estonia.com/e-residency-up-against-great-expectations.

[14] See Michael Tegos, Estonia's e-residency program makes it easy for Singaporeans to do business in the EU, TechAsia Feb 4, 2016 https://www.techinasia.com/estonia-e-residency-singapore-entrepreneurship.

[15] European Commission, Digital Single Market, February 25, 2016 at https://ec.europa.eu/digital-agenda/en/digital-single-market.

[16] Government of Estonia, "X Road Between Estonia and Finland, December 14, 2015 at https://e-estonia.com/x-road-between-finland-and-estonia/.

There are also broader collaborations, particularly with Singapore.[17]

E-Residency advances what until now has been essentially a national concept of digital identity, to a government-backed transnational digital identity that can be used across geographic borders for both private and public sector transactions. It is the first time that such a credential is not dependent on a person's legal entitlement through citizenship or physical presence in a country. As the Estonian government points out, Estonia is "one of world's most advanced digital societies. By providing e-Residency and opening up [its] services globally, Estonia is now moving toward the idea of a country without borders."[18]

E-Residency is a major development that brings forth unprecedented legal, policy, technical, and security issues. This paper explores the key features of e-Residency in the context of the application of blockchain to identity authentication, and their implications from a cross-discipline perspective.

2. Identity authentication for E-residency

> *"Starting in May 2015, it is possible to apply for e-Residency online and once the application is approved, just one face-to-face meeting is required to get the card."* [19]

As of 13 May 2015, e-Residency applications may be submitted online, not in person, as was initially the case.[20] Only one identity document such as a passport or national ID card is required to authenticate identity, and an applicant is only required to provide a photo or scan of that identity document when applying online. A photo of the applicant is required at the time of applying but an in-person interview is also no longer required.

After an application is received, the Estonian Police and Border Guard carry out a background check. Once cleared, the applicant attends a designated collection site outside Estonia to provide fingerprints and to collect the e-Resident ID card and card reader. The designated collection points are mostly at Estonian embassies and consulates. Although the plan was originally not to expand the number of pick-up sites,[21] a new site has recently been established in Singapore to meet demand in that area.[22] At that time, the applicant presents a photo identity document such as a passport and the applicant is fingerprinted.[23]

The online services currently available to e-Residents are also more extensive than expected this early in the establishment of the program. A company can now be incorporated and managed by an e-Resident online without any physical presence in Estonia and without the need to hire a local as a representative or involve an Estonian as a partner or co-director, for example.

E-Residents can also conduct banking online, including electronic transfer of funds,[24] access international payment service providers, and digitally sign documents. The Estonian government asserts that: "[T]he digital signature and authentication are legally equal to handwritten signatures and face-to-face identification in Estonia and between partners upon agreement anywhere around the world."[25] New digital authentication and document signing services for e-Residents are planned for 2016.

The Estonians also wish to enable an e-Resident to open a bank account without having to travel to Estonia. Banks in Estonia that recognize e-Resident smart ID cards[26] currently require an initial in-person meeting in order to open an account, but when the account is established e-Residents can then manage their banking and money transfers remotely, from anywhere in the world.

The requirement for an initial face-to-face interview is in line with the banks' obligations under Good Banking Practice, the Estonian banking code of practice,[27] and with Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) legislation, which was widely enacted around the world including in Estonia following the September 11 attacks on the United States of America.[28] The legislation mandates that banks

[17] "Singapore is one of our highest priorities [. . .] in terms of collaborating with developers and service providers in one of the top global startup ecosystems in the world," says Taavi. It is reported that there have been talks with Singapore's Media Development Authority and Infocomm Development Authority regarding collaborations between Estonia and Singapore. See Michael Tegos, Estonia's e-residency program makes it easy for Singaporeans to do business in the EU, TechAsia Feb 4, 2016 https://www.techinasia.com/estonia-e-residency-singapore-entrepreneurship.

[18] See, n 2 above.

[19] See, n 2 above.

[20] See, Government of Estonia, "Estonia opens e-Residency to the world", May 13. 2015, at https://e-estonia.com/estonia-opens-e-residency-to-the-world/.

[21] "You can pick up the card from our foreign embassies and consulates in 34 countries around the world, or at Police and Border Guard Board service points in Estonia. Please note that the Estonian honorary consuls do not issue e-Residency and we currently do not plan to expand the number of pickup locations."

[22] "Applicants will now be able to pick up their cards at regular "consular missions" that will take place every three months in Singapore. The first mission will be live in April for Singaporeans who get their applications in by March 1. According to Estonia's chief information officer (CIO) Taavi Kotka, a more permanent solution is in the works."

[23] "Once your application has been submitted, wait for the result of your background check, which should take about 10 working days. Once your application is approved, you will be invited to your chosen pick-up location to identify yourself, give fingerprints and collect your e-resident e-ID (it comes with a card reader). The whole process should not take more than a month, but may vary based on demand and pickup location." See, n 17 above.

[24] Although e-Residency does not necessarily expose an e-Resident to Estonian tax, where applicable an e-Resident can also pay his/her Estonian tax on-line.

[25] Ibid.

[26] Currently there are three banks in Estonia that recognize e-Residency – LHV, Swedbank and SEB.

[27] See, Good Banking Practice. Part 6 at http://www.pangaliit.ee/en/legal-acts/recommended-documents-of-eba/71-english/legal-acts. Although this is not legislation, as a code of practice it closely follows the KYC and STR requirements typically found in the AML/CTF legislation.

[28] See the Estonian Anti Money Laundering and Terrorist Financing Prevention Act Adopted 19.12.2007 RT I 2008, 3, 21 into force on 28.01.2008 at https://www.riigiteataja.ee/akt/13323731. Note that "the Estonian Financial Intelligence Unit (FIU) is an independent structural unit of the Estonian Police and Border Guard Board. Fi-

and financial institutions[29] check and report the identity of every customer. These Know Your Customer (KYC) requirements require that a person establish his/her identity to open a bank account and to undertake specified financial transactions. Significantly, the Estonian e-Residency team is working with a local startup, LeapIn, and Estonia's largest domestic bank, LHV, to allow the whole process to be done remotely using the e-Resident's e-ID and a video link enabling face-to-face real time interaction, to eliminate the need for an in-person meeting.

The current identity authentication process for e-Residency is much less rigorous than originally envisaged and it is generally less rigorous than identity authentication required to obtain a national digital identity in many countries. An applicant for Estonian e-Residence is not required to attend an in-person interview in Estonia or elsewhere. Moreover, the application only requires a scan of one identity document i.e. typically a passport or national ID card, rather than the range of identity documents usually required to establish identity under the KYC requirements. The Estonians are in effect 'piggy-backing' on the identity authentication process they assume has been undertaken to acquire the national identity document, rather than undertaking their own full identity check.

This approach is not generally in compliance with regulations and norms in the financial services sector. The full-check protocol established by the KYC procedures include an initial in-person interview, at which time the applicant provides a range of specified identity documents to satisfy the 100 point identity check which is now generally referred to as the KYC requirements. Originals, not copies or scans, of those documents are presented in-person by the applicant and copies of those documents are made at that time for the record. Not following this approach for e-Resident applications increases the potential for a person to obtain an e-Resident e-ID for financial transactions for which, depending on the national processes, has not necessarily been subjected to robust and independent checking and review per KYC norms and regulation. It increases the potential for an individual to obtain a new digital identity based on an inaccurate, falsified, or stolen passport or national identity card.

The process for collecting the smart ID card and reader outside Estonia is also not sufficiently robust, raising the potential for fraud and error at this stage too. The applicant must only present the identity document used for the application, and the applicant's appearance is compared to the photo uploaded for the application. That photo must meet specifications required by law in Estonia,[30] but there is potential for recognition error at the time of collection. In the case of a non-biometric photo comparison for example, recognition of a familiar face is reasonably robust. However, recognition of an unfamiliar face, as would mostly be the case at Estonian embassies and consulates abroad, depends on picture recognition. This involves matching of superficial features that is subject to error resulting in false positives as well as false negatives.[31] Research also shows that individuals are better at recognising and discriminating own-race versus other-race faces.[32] When identification is by comparison, there is opportunity for fraud, and greater likelihood of mistake.[33]

The applicant's fingerprints are also taken when he/she collects the smart ID card and reader. The purpose of biometrics is to link a person with the digital identity. At that time, the information used to register is linked with the person who collects the smart ID card and reader. If, however, that identity is based on inaccurate information or information which is not authentic to the person collecting the smart ID card, then that information will be connected to his/her fingerprints, thereby creating an apparently authentic and useable new digital identity.

3. The implications of Estonian E-residency

"Since the launch of e-Residency, we have received a vast amount of positive feedback. We have learned that people from around

nancial Intelligence Unit analyses and verifies information about suspicions of money laundering or terrorist financing, taking measures for preservation of property where necessary and immediately forwarding materials to the competent authorities upon detection of elements of a criminal offence." See, Government of Estonia, "Money Laundering Prevention" at http://www.fin.ee/money-laundering-and-terrorist-financing-prevention.

[29] And more recently other designated businesses susceptible to be used for money laundering. In Estonia, both KYC and suspicious transaction reporting (STR) requirements apply to credit and financial institutions, lottery and gambling institutions, real estate firms, high value goods traders, pawnbrokers, auditors and accountants, accounting and tax advisors, providers of trust fund and business association services and notaries, attorneys, bailiffs, and trustees and interim trustees in bankruptcy. See, the Payment Institutions and e-Money Institutions Act) passed 17.12.2009 RT I 2010, 2, 3 entry into force 22.01.2010 at https://www.riigiteataja.ee/en/eli/511112013017/consolide.

[30] See Requirements established for photos upon application for issue of documents [RT I 2010, 45, 272 - entry into force 01.10.2010] at https://www.riigiteataja.ee/en/eli/524092014025/consolide.

[31] Peter Hancock, Vicki Bruce and A Mike Burton 'Recognition of Unfamiliar Faces' (2000) 4(9) *Trends in Cognitive Science* 330.

[32] See, Clare Sullivan, Digital Identity (2010) discussing Pamela Walker and Miles Hewstone, "A Perceptual Discrimination Investigation of the Own-Race Effect and Intergroup Experience" (2006) 20(4) *Applied Cognitive Psychology* 461 and Kirsten Hancock and Gillian Rhodes, "Contact, Configural Coding and the Other–Race Effect in Face Recognition" (2008) 99 *British Journal of Psychology* 45. See also Jose Kersholt, Jeron Raaijmakers and Mathieu Valeton, "The Effect of Expectation on the Identification of Known and Unknown Persons" (1992) 6 *Applied Cognitive Psychology* 173, and, Sarah Stevenage and John Spreadbury, "Haven't we Met Before? The Effect of Facial Familiarity on Repetition Priming" (2006) 97(1) *British Journal of Psychology* 79.

[33] For example, in a study in which supermarket cashiers compared real people not known to them to photographs on the credit cards they presented, only 50 per cent accurately accepted or rejected the cards. When the card contained a photograph resembling the person presenting it, only 36 per cent of the cashiers correctly rejected the card. See, Richard Kemp, Nicola Towell and Graham Pike, "When Seeing Should Not Be Believing: Photographs, Credit Cards and Fraud" (1997) 11(3) *Applied Cognitive Psychology* 211.

the world see e-Residency as an opportunity to fulfil their dreams, venture across the borders, and become free from bureaucracy.”[34]

The significance of Estonian e-Residency should not be underestimated. The government of a sovereign nation state issues the e-ID issued to an Estonian e-Resident. Estonia is a full member of the EU. Registration as an e-Resident effectively creates a government-authenticated, transnational digital identity that one can use to remotely establish and run a business, open a bank account, transfer funds, and engage in trade.

The authenticity of this identity is crucial. An apparently official identity document, which has not been subject to robust checking, has been falsified or which is otherwise authentic but relates to another person,[35] can enable creation and use of new, false identities. A digital identity created in this way can then be used for a range of domestic criminal activities and international crimes ranging from fraud and money laundering to terrorism. In many ways, the Estonian e-Residency program provides an ideal vehicle for this type of activity because services can be accessed and used remotely.

Money laundering is a significant risk. Estonia plans to replace the in-person interview required to open a bank account with a video link enabling face-to-face real time interaction. Although the video interview required for opening a bank account may not be as secure and robust as an in-person interview, our main concern is the use of an inaccurate, inauthentic digital identity. That is why identity authentication at the time of registration and collection of the e-ID is so important. As to the other AML/CTF reporting procedures such as Suspicious Transaction Reporting (STR), banks in Estonia must comply with those requirements.[36] That reporting has strengthened detection of illegal activities and consequently has made financial transactions less attractive for laundering money. By contrast, many aspects of trade, especially over the Internet, are not regulated to the same extent, so trade is considered a relatively more viable option for criminal activity.

However, by far the highest risk in e-Residency lies in the potential to bypass traditional institutions and procedures, as suggested by Bitnation. This includes bypassing traditional identity authentication procedures conducted at the national level using government-backed checking processes, which effectively underpin identity authentication for Estonian e-Residency; and the AML/TF requirements, which apply to traditional financial institutions like banks but not to new virtual financing and payment methods like bitcoin,[37] nor to all trade in goods and services.[38] An easily obtainable transnational digital identity that enables unreported and unmonitored trade and commerce is the ideal vehicle for fraud, tax avoidance and money laundering. Money laundered in this way can then be used to fund crime and terrorist activity domestically and internationally.

In November 2015, Estonia announced it is collaborating with Bitnation, one of several emerging initiatives based on blockchain technology, which are specifically designed to bypass traditional, national governance systems. Blockchain is the technology that underpins Bitcoin,[39] a virtual peer-to-peer currency and payment system that enables users to transact without using a traditional intermediary such as a bank or government department or agency. In its broadest application, this technology aims to provide a new system to vouch for the integrity of identity outside governmental structures, for contractual agreements for banking and company incorporation, and for new payment systems outside the traditional finance sector. The underlying philosophy is that identity is established using a distributed ledger on a global open source platform, rather than using traditional authentication sources like government records and authentication intermediaries like banks, for example.

This potential use of blockchain for identity and for at least some transactions for Estonian e-Residents is a significant development that will ostensibly enable the provision of self-sovereign identity and other related services to e-Residents. As the joint press statement points out, “[v]ia the international Bitnation Public Notary, e-Residents, regardless of where they live or do business, will be able to notarize their marriages, birth certificates, business contracts, and much more on the blockchain.” [40]

4. The implications of Estonian E-residency using blockchain

“In Estonia we believe that people should be able to freely choose their digital/public services best fit to them, regardless of the geographical area where they were arbitrarily born,” said e-Residency Program Director Kaspar Korjus. “We're truly living in exciting times when nation states and virtual nations compete and collaborate with each other on an international market, to provide better governance services.” [41]

[34] Katre Kasmel, Head of communications for e-Estonia as reported in Justin O'Connell, “Interview: Estonia Doesn't Think you Know how Awesome e- Citizenship is Yet” at https://hacked.com/interview-e-estonia-doesnt-think-know-awesome-e-citizenship-yet/.

[35] The present Syrian refugee crisis in Europe has highlighted the trade in fake and stolen identity documents. Reportedly, non-Syrians are using Syrian identity documents that are stolen or forged, in whole or in part, in order to claim asylum. See, Nick Fagge “Germany is ‘overwhelmed’ with false asylum seekers' Syrian passports as forgery experts admit they can't spot fakes” The Guardian, 5 November 2015. See also, Giulia Paravicini, “EU's Passport Fraud ‘Epidemic’”, Politico, 28 January 2016.

[36] See, n 28 above. See also, the Payment Institutions and e-Money Institutions Act) passed 17.12.2009 RT I 2010, 2, 3 entry into force 22.01.2010 at https://www.riigiteataja.ee/en/eli/511112013017/consolide.

[37] Although the Payment Institutions and e-Money Institutions Act also applies and attempts to regulate e- money institutions, as a matter of law and practicality it does not clearly apply to virtual currency and payment systems like Bitcoin, for example.

[38] See https://bitcoin.org.See also n 28 above.

[39] See https://bitcoin.org.

[40] Government of Estonia Press Release, “Starting December 1, 2015 the Estonian e-Residency program, in partnership with the virtual nation BITNATION.co will use Blockchain Technology to offer a Public Notary to e-Residents”, November 26, 2015 at https://bitnation.co/blog/pressrelease-estonia-bitnation-public-notary-partnership.

[41] Ibid.

The e-ID issued to e-Residents is the next evolution of digital identity, moving identity from a national concept to a transnational one. The application of blockchain technology takes this evolution to an unprecedented level, by enabling individuals to control access to their identity information,[42] and to create, manage and use a self-sovereign identity. This type of distributed ledger system also has broader application to financial services, real estate, and healthcare for example, though there are substantial questions as to the type of information that should be stored and accessible on blockchain.[43]

In the context of identity, blockchain is said to be able to prove a person exists at a certain time and place, based on verification by a group of people. In effect, their consensus constitutes reality. In other words, if the consensus is that it is so then it is so.

A block chain is a public ledger distributed across many computers. In essence, blockchain technology provides non-repudiation of time-ordered events by a group of distributed servers, usually under the control of different people, usually in different locations and preferably in different countries. Participants within the network have their own copy of the ledger. Changes to the ledger are public and broadcast to all participating nodes. Changes to the ledger effectively appear in all copies. Although each ledger may not have each and every event recorded, they can, with certain guarantees based on proof of work and the likelihood of an attacker being able to perform that work independently of the network, be able to verify the order of events. The security and accuracy of the information stored in the ledger are maintained cryptographically.

Through the use of keys and signatures to control who can do what within the shared ledger, one can expand the use of blockchain technology beyond its first use case, financial transactions. According to rules agreed to by the network, one, some or all of the participants, can add entries that update existing entries. Blockchain algorithms aggregate transactions in 'blocks,' and those blocks are added to the chain of existing blocks, using a cryptographic signature that includes a proof of work. The proof of work makes it cryptographically unlikely for an attacker to alter prior blocks. The public nature of adding new blocks makes it hard to get a false block accepted by the network.

There are questions about the scalability of blockchain systems, especially for worldwide and even regional use. For example, scalability is a reportedly an issue for Bitcoin, the first application built on top of blockchain, with reports that the chain it is reaching capacity, though it should be also noted that there are also reports to the contrary.[44]

Bitnation is an implementation of blockchain technology to provide identity, reputation, and dispute resolution services, as well as public registries for insurance, security, marriage, death certificates, and land titles.[45] According to Susanne Templehof, founder of Bitnation, the broad objective of Bitnation is "to gain recognition for Bitnation as a sovereign entity, thus creating a precedent for open source protocol to be considered as sovereign jurisdictions."[46] This in effect seeks to "establish a new virtual jurisdiction with its own rules".[47]

[42] G Zyskind, O Nathan, A Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", in 2015 IEEE Security and Privacy Workshops, 21–22 May 2015, 180–184.

[43] See, Mike Gault, "Forget Bitcoin – What Is the Blockchain and Why Should You Care?" ReCode July 5, 2015 retrieved from https://web.archive.org/web/20160130030819/http://recode.net/2015/07/05/forget-bitcoin-what-is-the-blockchain-and-why-should-you-care/.

[44] See for example, Mike Hearn, "*Bitcoin Network Reaching Critical State*" CCN LA, 6 May 2015 at https://www.cryptocoinsnews.com/bitcoin-network-capacity-reaching-critical-state-mike-hearn/. However see also, Jacob Donnelly, "*Here's what the future of bitcoin looks like – and it's bright*", Crypto Brief, Venture Brief, 14 February 2016 at http://venturebeat.com/2016/02/14/heres-what-the-future-of-bitcoin-looks-like-and-its-bright/. In any event, technological solutions will almost certainly eventually be developed to address capacity issues.

[45] Bitnation describes itself as "a decentralized, open-source movement, powered by the Bitcoin blockchain 2.0 technology, in an attempt to foster a peer-to-peer voluntary governance system, rather than the current 'top-down', 'one-size-fits-all' model, restrained by the current nation-state-engineered geographical apartheid, where your quality of life is defined by where you were arbitrarily born." In further detail Bitnation states that it "provides the same services traditional governments provides, from dispute resolution and insurance to security and much more – but in a geographically unbound, decentralized, and voluntary way. Bitnation is powered by Bitcoin 2.0 blockchain technology – a cryptographically secured public ledger distributed amongst all of its users. As we like to say – Bitnation: Blockchains, Not Borders." See Bitnation Governance 02 at https://bitnation.co/join-the-team.

[46] According to Bitnation CEO and founder Susanne Templehof as reported in Ian Alison, "Bitnation and Estonian Government start Spreading Sovereign Jurisdiction on the Blockchain," 28 November 2015 at http://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923. Bitnation has recently received international attention for providing assistance to Syrian refugees in Europe including an emergency digital identity and financial services through a Bitcoin Visa card to enable a refugee who cannot establish a bank account to receive funds from family, for example. Blockchain is used to cryptographically establish an individual's existence and family relations to generate a digital identity. That identity generates a Quick Response Code, an optical label that contains information in machine-readable form that can be read by a mobile phone to apply for a Bitcoin Visa card which can be used throughout Europe without a bank account. Susanne Templehof, founder of Bitnation, reportedly explained that "the Blockchain Emergency ID is a rudimentary emergency ID, based on the blockchain technology, for individuals who cannot obtain other documents of identification." She explains, "[w]e are providing emergency ID and then this visa card because most refugees will be unemployed. They won't be legally able to get a job for several years and they can't open a bank account." See Ian Allison "Decentralised government project Bitnation offers refugees blockchain IDs and bitcoin debit cards" International Business Times, October 30, 2015 at www.ibtimes.co.uk/decentralised-government-project-bitnation-offers-refugees-blockchain-ids-bitcoin-debit-cards-1526547. Use of blockchain in this type of situation to create an emergency, temporary digital identity to enable aid to be given to an individual who is unable to otherwise establish his/her identity may be admirable. However, it does raise security concerns particularly in the use of this means to create and new, false identity and to engage in nefarious and covert activity ranging from crimes like money laundering to activities endangering national and international security.

[47] Ibid. As well as the huge increase in stateless people in Europe from the refugee crisis, Bitnation is looking at developing markets, assisted economies and the grey economy. For example the reg-

Templehof provides the example of marriage between a same sex couple which is not recognized as legal in a number of countries but is possible using Bitnation. "[T]o get married on the blockchain would take you ten minutes between writing the contract and time-stamping it." She points out that "you could marry as many people as you want, any gender." Templehof warns, however, that "the intrinsic immutability of blockchain systems means it could be very hard to get a divorce, suggesting short term marriage contracts of four or five years at a time."[48] There are already indications of the role of e-Residency in this process. E-residency team product manager Ott Vatter cites the example of a Spanish couple who obtained their Estonian e-Residency for the purpose of registering a marriage on the Bitnation blockchain.[49]

The use of blockchain in this way raises the potential to create an identity outside traditional national and international channels. For example, a name change can be affected through a marriage recorded on Bitnation. That new name could then be used to register a digital identity under a national identity registration scheme like that being implemented in India, for example. This enables creation of a new digital identity and in effect, a new legal identity, which in reality is without lawful basis and which could be used to hide real identity.

The main advantages of Bitnation's implementation of blockchain are individual empowerment and the potential for improved security. Security is improved largely because the identity documents are stored on, and authenticated by, the distributed ledger rather than having multiple copies stored on government and proprietary systems. In the distributed ledger, a record of the authorization is stored in the chain and that is touted as improving security by providing attribution and accountability. It is an improvement in some respects. However, it should be noted that access can be tracked and proved without blockchain, though less easily. If there is a deliberate cover-up for example, this information may need to be found forensically which can be difficult, time consuming, and costly.

This all said, it should be noted that Bitnation is not a sovereign nation and as of the time of this writing has no legitimacy in law. That is, none of the transactions registered by Bitnation have any legal standing, unless also recognized by a real sovereign nation. For example, no one will recognize a 'wedding' registered at Bitnation that is not also recognized by some other state. Note that this occurs between real states as well. For example, a marriage between two men in the Commonwealth of Massachusetts is recognized in the United States but will not be recognized in the Russian Federation. The difference is, as of now, no national will recognize a marriage registered by Bitnation.

5. The security implications of blockchain in the context of Estonian e-residency systems

> *"Estonia continues to be one of the most digitally advanced countries, using blockchain technology to keep citizen's data safe is another example of the country's forward thinking."*[50]

The Estonian government is on record stating that "[p]rocedures and practices are in place to ensure the safety of e-Residents' data and limit ways for misuse."[51] The e-Resident e-ID and services use a rooted Certificate Authority (CA) chain of trust. Most browsers around the world have the Estonian root CA certificate pre-populated. This means that identities signed by Estonia will validate on most systems. The challenge for Estonia is getting the world user community to recognize identities signed by Estonia to be valid. The ease for Estonia is the precedent of Extended Validation Certificates; most users are unaware of who signs the root for certificates, and as such will blindly accept certificates issued by Estonia as valid for commercial transactions. As well, Estonia is doing a good job educating the Internet public that these certificates are good for more than just signing or encrypting a Web site or an email message.

For people to accept an Estonian digital identity as legitimate, they need to have assurance that Estonia only issues the identity to those whom it knows. This is the purpose of the initial vetting that Estonia performs before issuing an e-Residency card.

For general acceptance, people also need assurance that it is not easy to forge or compromise issued certificates. To this end, Estonia uses 2048-bit public key encryption for its certificates. As well, access to the certificates is through hardware devices that are difficult to compromise. In the case of the e-Residency card, it is a secure smart card combined with a secure card reader that requires the user to enter a pin. An attacker that acquires someone's card still cannot use it without the PIN and reader. Moreover, the card is effectively impossible to clone.

There is an additional risk with using a root certificate authority approach to issuing digital certificates. It is that few applications verify which root certificate authority signed the certificate. What this means is someone other than the Estonian government can sign a certificate claiming to be an Estonian e-Residency ID. This is an example of the attack on Google, when DigiNotar was hacked and certificates with claims of "google.com" were used, presumably by Iran to deceive dissidents within the country as well as to collect intelligence outside the country.[52] What limits the abuse of this technique is if a certificate authority is known to issue false certificates, the community quickly bans them. For example,

istry capabilities of blockchain are being considered as a means of recognising land rights in the developing world in countries like Ghana, where 70% of land is reportedly untitled and land is traded peer to peer.

[48] See n 46 above.

[49] See n 10 above.

[50] Government of Estonia, "Guardtime Secures Estonian Health Records" March 8, 2016 at https://e-estonia.com/guardtime-secures-estonian-health-records/.

[51] The Government of Estonia, "What is e-Residency" at https://e-estonia.com/e-residents/about/.

[52] Fox-IT BV, *Operation Black Tulip*, at https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf.

even though DigitNotar was the victim of a hack, they went bankrupt.[53]

There are technologies, such as certificate pinning, that either notify the user when there is an attempt to use a different root certificate than was used in a prior session or, for high security applications, the application will only trust a single certificate authority.

This is symptomatic of a currently unsolved problem with the principal of certificate authorities: that in countries like the United States, the root of trust for a CA is vested in the market rather than in irrefutable measures of trust, and anyone can become a CA. However, because its government backs Estonia's e-ID CA, the Estonian e-Residency program can overcome this aspect of the Certificate Authority root of trust problem if trust is properly and independently established when issuing e-IDs.

A blockchain approach such as Bitnation attempts to eliminate the root of trust problem. This is because instead of a central authority for being the root for certificates, blockchain distributes the ledger amongst hundreds or thousands of servers under different administrative control. There is still a bootstrap problem of finding an initial blockchain ledger server that is trusted, but presumably, there will be many with their identities published and publicly available for inspection. As such, it is unlikely for an adversary to be able to corrupt the root of the blockchain.

However, while the new application of blockchain to identity authentication has considerable potential advantages in facilitating national and international interoperability, there are other concomitant risks, particularly in enabling creation and use of new, false identities, illegal use of legitimate identities, and in facilitating illicit activities ranging from organized crime, to terrorist organization and funding. This is particularly so if this technology is used to enable identity information to be authenticated and used outside existing law applying in sovereign states.

Although general statements by Tempelhof indicate that this is the broad objective of Bitnation, her comments in relation to the collaboration with Estonia are more moderate: "[m]y aim is to see a world where hundreds of thousands or millions of governance service providers in a free global market competing through offering better services at a better value, rather than through the use of force within arbitrary lines in the sand." "To that end, seeing nation state governments starting to provide governance services on a free global market as well, like The Republic of Estonia, is encouraging, and a step in the right direction. Now we need more nation state governments, as well as open source protocols joining the global market."[54]

Indeed, a more realistic approach is to harness the benefits provided by blockchain and integrate this new application to exiting legal and procedural standards, especially the established national and international frameworks such as the KYC and STR requirements. It is not clear yet whether this will be the approach adopted by the Estonians in their collaboration with Bitnation, but it is most likely. It is the most feasible option because it clearly has legal basis under Estonian law and under international law; and for that reason is likely to be more acceptable to the international community and law-abiding e-Residents. It is important to bear in mind that although 'facts' are recognized within the blockchain as being valid, they are not legally binding.

There is precedent for using blockchain to support existing legal requirements in the Isle of Man where collaboration between government and private enterprise resulted in the use of distributed ledgers for identity authentication under the existing KYC system.[55] In this application, blockchain is used by "taking the source data from the passport office, from the DMV, from the post office, from the utility companies, and using that to prove granular things about a person's identity".[56] This is the next evolution of what generally occurs now in decentralized government systems and in the case of KYC checking, the process whereby a scan of a passport, utility bills and other supporting documentation required to establish identity, are taken from originals and uploaded, to fulfill the AML/CTF requirements. This type of distributed ledger can be developed within existing national frameworks, but there is also considerable scope for transnational identity authentication both regionally such as within the EU, and more broadly as is necessary for e-Residency.

When used in this way, blockchain can have considerable benefits, especially for an individual by providing him/her with greater control, and protection identity information and documentation. For example, instead of organizations like the Estonian Police and Border Guard and intermediaries such as banks, each uploading and storing a scan of a passport and other supporting documentation required to authenticate identity, blockchain could be used. In this way, it can operate as a more efficient and secure form of public key infrastructure, directly authenticating the source data from the passport office or other government departments and utility companies. It is more secure because copies of crucial identity documents, such as a person's birth certificate and passport, are not stored on a number of databases, and consequently, are not as susceptible to unauthorized access and misuse.

It should be noted, however, that although this application of blockchain is more acceptable, it is still new. While blockchain is touted as being more secure than existing systems

[53] It should also be noted that the hack and bankruptcy of DigiNotar set back the Dutch plans for electronic government. For example, the business appeals court of Den Haag stated in 2011 that they had to move to an SMS, 2-factor authentication system as a result of not being able to trust DigiNotar-signed certificates. See https://www.rechtspraak.nl/SiteCollectionDocuments/Jaarverslag-2011-CBb.pdf, 6.

[54] Giulio Prisco, "Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents" Bitcoin Magazine, December 1, 2015 at https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243.

[55] The world's first government block chain application was implemented in the Isle of Man in 2015. See Interview with Credits CEO and Co-Founder Nick Williamson, Credits, 15 December 2015 at http://www.credits.vision/posts/interview-with-credits-ceo-co-founder-nick-williamson.

[56] Ibid.

and that appears to be borne out in its use for Bitcoin,[57] it is more widespread use for identity may reveal new security vulnerabilities. For example, even though one could rely on an underlying attestation is genuine when an individual supplies, for example, a passport with a number that can be verified, the entity may still have the temptation (or misguided regulations may demand) to keep a copy of the document. This subverts one of the presumed advantages of blockchain that enterprises will not need to keep their own copies of documents, which present their own risks of loss.[58]

Individual control, which is a feature of some blockchain implementations, raises issues about the authenticity of the documents and information he/she places on the chain. The use of blockchain for identity is untested and it raises issues as to responsibility of those who vouch for the accuracy of the information and for the ensuing consequences of relying on that information.

The legal implications can be complex. The applicable law depends on the type of system, e.g. whether the blockchain is owned and operated by government, whether all of it is privately owned but used by government, and the location and control of the blockchain ledgers.

6. The implications of blockchain for data protection regulation

> *"e-Residency offers to every world citizen a government-issued digital identity and the opportunity to run a trusted company online, unleashing the world's entrepreneurial potential."*[59]

Estonia is a member of the EU and is subject to EU law, including data protection requirements. The identity documents and information located on the chain is "personal information" as defined in the 1995 Data Protection Directive (1995 Directive) and in the new General Data Protection Regulation (GDPR) which will replace the Data Protection Directive 95/46/EC (1995 Directive)[60] in the EU in April 2018. As a Regulation, the GDPR directly applies in a Member State,[61] in contrast to a Directive where each Member State has discretion as to how to incorporate its requirements into national law.

Like the 1995 Directive, the GDPR sets out requirement for of natural persons with regard to the processing of their personal data. The GDPR is in substantially same terms as the 1995 Directive but updates the Directive and expands jurisdictional scope. Whereas the 1995 Directive applied to processing of personal data in the EU, the GDPR applies to processing personal data of EU data subjects,[62] wherever that occurs.[63]

The GDPR defines "personal data" simply and broadly in Article 6 as "any information relating to a data subject."[64] Article 6 defines "data subject" as "an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller[65] or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." [66] This definition is similar to the definition of 'data subject' in the 1995 Directive, but although the GDPR retains the direct and indirect identification requirement, the GDPR includes "means reasonably likely to be used" by any natural or legal person in identifying a data subject. The new definition also goes beyond 'identification number' specified in the 1995 Directive, to also include "location data" and "online identifier."

Locating identity documents and information on blockchain is clearly "processing" and the individual e-Resident is the "data subject" as defined under both the 1995 Directive and the GDPR. An EU citizen for the purposes of the 1995 Directive and the GDPR is a resident of the EU i.e. a person who has a substantial physical presence or physical connection with a member country. This excludes Estonian e-Residents who are not EU residents under this definition.

Even when an Estonian e-Resident is an EU resident, the protection provided by the 1995 Directive and the new GDPR is limited, even though under the Regulation data protection

[57] However for a recent security issue with another virtual currency see, Rob Price, "Digital currency Ethereum is cratering because of a $50 million hack" Business Insider Jun 17, 2016 at http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6.

[58] One cannot lose information that one does not have.

[59] Estonian government, "What is e-Residency?" at https://e-estonia.com/e-residents/about/.

[60] Recital (171) of the GDPR explains that Directive 95/46/EC is repealed by this Regulation and states that "[P]rocessing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed."

[61] Unless a member state is exempted. The GDPR comes into effect in April 2018 after a 2-year transition period.

[62] Under the GDPR, an EU data subject is a data subject in the EU.

[63] The GDPR applies to processing personal data of a EU data subject regardless of the data controller's place of incorporation, geographical base and area of operation under Article 3.

[64] See Article 4 of the New Regulation.

[65] See, Article 4 (7) of the new Regulation.

[66] To be considered personal data as defined, the data and information must relate to a living person. See for example, Efifiom Edem v Information Commissioner and Financial Services Authority [2014] EWCA Civ 92, (Efifom) where the English Court of Appeal held that when determining whether a person's name is personal data, the question is whether the data identifies a living individual. This decision clarifies the earlier requirement established in Durant v Financial Services Authority [2003] EWCA Civ 1746 (Durant) that information must be sufficiently biographical to constitute personal information. While that part of the judgment has been overturned, Durant points out that the information "should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest". See Durant v Financial Services Authority [2003] EWCA Civ 1746, ¶ 28.

requirements nets will be essentially uniform across the EU. Estonia is exempted from the requirement to impose significant new penalties for breach of Article 6 of the GDPR,[67] which covers lawful processing of personal information. More importantly, the disruptive nature of blockchain does not sit comfortably with data protection requirements under either the 1995 Directive or the GDPR. The possibility for individual control is a feature of the blockchain model. In that respect blockchain is considered to have an advantage over existing systems because the individual could be responsible for placing information on the blockchain and for controlling access. However, this raises the interesting point that the individual can be both data controller and data subject as defined under the 1995 Directive and the GDPR, rendering many of the data processing requirements a nonsense.

This is also an issue for data protection regimes in countries outside the EU that have adopted the EU model. Data protection legislation and practice in jurisdictions as diverse as the African Union, Singapore, Mexico, Japan and Australia for example, have based their data protection regime on the EU model, particularly on the 1995 Directive. The reasons are pragmatic. The EU requires that countries wishing to do business with the EU have data protection to the same standard; and the 1995 Directive provides a model, which has been widely adopted.

The EU data protection requirements are highly influential in shaping data protection law internationally so it can be expected that the EU will continue to set the standard for data protection, and that the changes made by the GDPR, especially its broadened extraterritorial application, will similarly continue to inform law reform outside Europe.

Australia is indicative of the wider international adoption that can be expected in extending the territorial reach of data protection requirements. Like the EU, Australia has extended the territorial reach of its Privacy Act 1988 (Cth), though it did so before the EU and in a more effective way. Australia was one of the first nations outside Europe to implement data protection legislation based on the EU model and over time, Australia has updated the Privacy Act to align with EU requirements to facilitate business with the EU. In 2014, major amendments were made to the Act including to the regulation of the processing of cross-border data. The reform created a new single set of "Australian Privacy Principles" ("APPs") that updated and consolidated the separate set of principles that previously applied to government agencies and private sector entities. A number of APPs introduced significant change.

The most significant from an international perspective is the new APP 8, which regulates cross-border disclosure of information. Regulating disclosure, rather than transfer, widens the scope of APP 8, both in terms of the activities it covers and the entities to which it applies. Under APP 8, an Australian entity can disclose personal information to an overseas recipient if it takes such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information. In certain circumstances, an Australian entity can be deemed liable for breaches of the Privacy Act committed by the overseas recipient. The only way an entity can escape the effect of this deeming provision is to rely on one of the relatively narrow exceptions specified in the Act, which includes consent of the data subject. APP 8 requires that the entity obtain individual consent after having clearly and unambiguously set out how at the information is, or may be, disclosed. In the absence of consent of the data subject, the entity must ensure that information is protected to the same standard, as it would be in Australia.

Like the new GDPR, this approach seeks to extend the international reach of national data protection standards. In addition, like the 1995 Directive and the GDPR, the Australian Privacy Act could be rendered ineffective by blockchain if the same person is both data subject and data controller as defined under the legislation.

7. Blockchain and the right to identity under international law

> *"E-Residency enables everyone, everywhere to securely identify him or herself online, open and run a location independent business, and take advantage of a marketplace of services specifically for e-residents."*[68]

The full legal implications of blockchain are not yet known. It is clear though, that use of a distributed ledger raises new legal issues regarding responsibility for the documents and information stored and accessed on the ledger, and for the ensuing consequences in the event that their accuracy, integrity and security is compromised. This is so even though Bitnation is attempting to position itself as a virtual sovereign entity outside exiting law.

The collaboration of Estonia with Bitnation for the e-Residency program will be subject to contract and hence to national law.[69] Estonian law governs the e-Residency program and Estonia is subject to international law. This is significant in the context of identity because while national data protection legislation is largely incapable of effectively applying in the blockchain context, an individual right to identity exists under international law. In the absence of effective data protection nationally for e-Residents, this right to identity is of increased significance.

The right to identity is a fundamental human right that arises at birth under the Convention on the Rights of the Child (CRC)[70] to which Estonia is a signatory. A right to identity is expressly included in Article 8 and the CRC distinguishes the right to identity from the right to privacy in Article 16. Article 8 was included in the CRC as the result of a campaign by the grandmothers of 'The Disappeared' in Argentina for the right

[67] The Netherlands is the other member state exempted.

[68] The Government of Estonia, "Crowd Valley Integrates e-Residency Platform to Enable Fully Digital Finance Services", June 2, 2016 at https://e-estonia.com/crowd-valley-integrates-e-residency-platform-to-enable-fully-digital-finance-services/.

[69] It is usual for the contract to specify the governing law.

[70] Adopted and opened for signature, ratification and accession by United Nations General Assembly resolution 44/25 of 20 November 1989, (entered into force 2 September 1990, in accordance with article 49). Estonia's adherence date is October 21, 1991.

to identity[71] who argued that hat that country's s adoption laws enabled concealment of children's true identities and the creation of false identities.[72]

Under article 8 (1) of the CRC there is an express right to identity and although the CRC is confined to rights of minors, considering the nature of the right to identity, arguably it continues when a child becomes an adult. The argument that a right to identity for all be recognized, has now been considerably strengthened by the formal adoption by the United Nations General Assembly of Sustainable Development Goal 16.9 which provides that member states provided a "legal identity for all, including birth registration" by 2030. [73],

In the EU, the European Court of Human Rights (European Court) under Article 8 of the European Convention Protection of Human Rights and Fundamental Freedoms (ECHR) has recognized the right of both minors and adults to identity.

The right to identity can also be recognized under the International Covenant on Civil and Political Rights (ICCPR),[74] particularly under Article 1(1):

> *"All peoples[75] have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development."[76]*

The CRC and the ECHR can provide the basis for legal action by an individual[77] whose identity information is not accurately recorded or which has not been adequately protected on blockchain, but the ICCPR potentially has greatest impact on state conduct through the monitoring of national implementation of the ICCPR by the United Nations Human Rights Committee (UNHRC).

The right to self-determination under Article 1 of the ICCPR is generally considered to be in-line with the international legal meaning of self-determination,[78] and to cover both the internal and external aspects of the right.[79] While the external aspect has in areas other than colonization[80] not been the subject of analysis, arguably it can ostensibly apply to digital identity.

Self-determination under Article 1 of the ICCPR invokes protection of the "private sphere" as advocated by Charles Reich.[81] Reich calls "the individual sector" the "zone of individual power'" necessary for the healthy development and functioning of the individual and "absolutely essential to thehealth and survival of democratic society".[82] A right to identity is part of that personal sphere, and arguably it now includes the right to digital identity. Digital identity is protected under Article 1(1) of the ICCPR because the Article protects individual autonomy and that is directly relevant to the use of blockchain for identity authentication, especially considering that it purports to give the individual control over his/her identity information and who can access it.

The UNHRC refuses to examine individual complaints based only on Article 1.[83] However, nations including Estonia must report to the UNHRC regarding implementation of Article 1 of the ICCPR and this reporting is the most effective part of overseeing compliance. Because countries that have ratified the ICCPR must report every 4 years. The UNHCR publishes its findings, identifying any areas of concern. These "concluding observations," by the UNHRC are a significant moral and political obligation for a government like that of Estonia which has committed itself to complying with the treaty.

[71] See Sharon Detrick, "*The United Nations Convention on the Rights of the Child. A Guide to the "Travaux Preparatoires"*"(1992), 292.

[72] Their campaign led to Argentina recognising a constitutional right to identity. See Lisa Avery, "Return to Life: The Right to Identity and the Right to Identify Argentina's "Living Disappeared"" (2004) 27 *Harvard Women's Law Journal* 235.

[73] See, United Nations, "Transforming our world: the 2030 Agenda for Sustainable Development" at https://sustainabledevelopment.un.org/post2015/transformingourworld.

[74] Adopted by the United Nations General Assembly Resolution 2200A (XXI) of 16 December 1966,entered into force on 23 March 1976, in accordance with article 49, for all provisions except those of article 41; 28 March 1979 for the provisions of article 41 (Human Rights Committee), in accordance with paragraph 2 of article 41. Estonia's adherence date is October 21, 1991.

[75] The HRC has confirmed that Article 1 (1) of the ICCPR applies to all peoples not just colonised peoples. See, Commentary on Azerbaijan 1994 UN doc CCPR/C/79/Add.38.para 6.

[76] The International Covenant on Economic, Social and Cultural Rights contained an identical provision. See, International Covenant on Economic, Social and Cultural Rights. adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entered into force 3 January 1976.

[77] The treaty obligations as standards may form the basis of legal action under national law or in the case of ECHR action may be taken under the treaty itself, though it should be noted that human rights claims have different objectives and standards of proof from typical damages claims. The former are designed to regulate state conduct and standards in upholding individual human rights whereas the latter are primarily designed to compensate for damage caused, though usually the is a consequential impact on conduct and processes.

[78] See, however, McCoddrick, D, *The Human Rights Committee* (1993), 248.

[79] The HRC has not clearly defined "self-determination" in Article 1. CERD has identified an internal and an external aspect. The internal aspect as defined by HERD is "the rights of all peoples to pursue freely their economic, social and cultural development without outside interference. In that respect there exists a link with the right of every citizen to take part in the conduct of public affairs at any level." CERD states that "the external aspect of self-determination implies that all peoples have the right to determine freely their political status and their place in the international community based upon the principle of equal rights." See, CERD, General recommendation 21I on the right to self-determination, adopted 23 August 1996.

[80] However, the exact meaning and application of Article 1 is open to interpretation. See, CCPR General Comment No. 12 [21]: The right to self-determination of peoples (Art. 1), adopted on 13 March 1984 and CERD General Recommendation No. 21.

[81] See, Charles Reich, "The Individual Sector" (1990–1991) 100 *Yale Law Journal* 1409.

[82] Ibid 1442, as quoted in Clare Sullivan, Digital Identity (2010).

[83] Although it has been criticized for this view, the HRC considers that that only individual rights recognized in Part III of the ICCPR (articles 6 to 27) can be examined under the individual complaints procedure established by the Optional Protocol to the ICCPR, adopted and opened for signature and accession by General Assembly resolution 2200 A (XXI) of 16 December 1966. t.

8. Conclusion

> *"A digital identity itself does not bring along new risks (e.g. money laundering). Instead, it makes existing risks more visible and manageable, as digital footprints are easily traceable – although we will make use of it only upon suspicion. We also check the background of applicants to make sure we can trust them as future e-residents."* [84]

The Estonian e-Residency program is a significant development. In many respects, it heralds the near future and is the model for other countries and regions, including the EU, which are pursuing a similar digital agenda. However, while there are major benefits now and in the future, there are accompanying risks that are largely dependent on the rigor of processes for authenticating identity.

In requiring only one identity credential, e.g. passport or national identity card, the current identity authentication required for e-Resident applicants does not meet the international standard set by the AML/CTF requirements. The Estonian e-Residency application process departs from that standard in three respects: by no longer conducting a face to face in-person interview with the applicant, by not requiring production of a range of original documents[85] to substantiate identity, and lastly by only requiring a photo or scan (and not sighting the original) of the identity document used for the application. The plans for requiring this process for opening a bank account also breaches this international standard, Estonian law, and commonly accepted banking standards.[86]

As a consequence, the e-Residency program now clearly raises concerns about identity crime and fraud, with the most significant risk being the use of e-Residency and its services for money laundering. Trade-based money laundering by organized crime and terrorist organizations is a major concern.

Using blockchain for e-Residency could fundamentally change the way identity information is controlled and authenticated. Blockchain technology provides decentralized, cryptographically signed proof of existence. This new application of blockchain offers the potential for individuals to control access to their identity information. In theory, an individual can provide access to select parts of their identity information, and documentation and the blockchain provides greater security. These are significant benefits to blockchain that, like e-Residency itself, herald the near future in identity management and authentication, but as yet its application is untested and the ensuing implications are not fully known.

It is clear however, that although Bitnation notary services like those to be offered to Estonian e-Residents are recognized within the blockchain as being valid, they are not necessarily legally binding in the Estonian jurisdiction, nor in any other nation state. Moreover, there is the risk that identity information authenticated on the blockchain but which is otherwise invalid may find its way into traditional channels[87] to enable creation of new, false identities, which could then be used to hide one's real identity. Apart from concerns about illicit activity that this may shield, if identity authentication is compromised in this way, it could substantially undermine the integrity and reliability of a national identity scheme or a transnational identity scheme like Estonian e-Residency. It is important therefore that the notary services using blockchain are located within the exiting legal framework, not outside it.

Acknowledgement

The authors thank Robert Ramirez for his comments and assistance in the preparation of this paper. The Army Research Office provided funding for this paper through the Minerva Initiative agreement # W911NF-15-1-0595.

[84] Ibid.

[85] As required for the KYC check, formally known as the 100-point identity check.

[86] Late in 2016 after this paper was written, Estonian banks announced new restrictions on non-residents opening bank accounts, reportedly "to combat money laundering" See https://1office.co/estonia/blog/opening-bank-account-estonia-non-residents. However, see also Government of Estonia, "Banking for e-residents: Your key questions answered" at https://medium.com/e-residency-blog/banking-for-e-residents-your-key-questions-answered-99519bb28d85.

[87] Even robust checking can be subject to machine and human error.