

---

# APPLYING BLOCKCHAIN TO IDENTITY

In my final deep dive into blockchain use cases, I come to digital identity. Now this is a thorny area for three reasons.

244

Shares

First, we need to understand what we mean by identity before we can talk about how blockchains could help.

178

55

Second, we need to understand the difference between blockchain and shared ledgers which, for digital identity, is a fundamental difference. This is why identity scheme experts get angry when people talk about blockchain solving digital identity for, as you will see, blockchain is not the solution.

Third, as with clearing and settlement, identity schemes are more related to industry and government structures than technology. Identity schemes are not a technology issue but a structural one.

For these three reasons this is a very long blog update – almost 4,000 words – and I'll start with the third point first. Right now there are several structural schemes under way to try and address the management of identities online. Some, like those in the Nordic region, are government and industry working together to create digital signatures and identities. Others are getting plaudits because they have set the standard, such as the Estonian government's scheme.

The Estonian scheme is important as it is the first program to realize the vision where citizens control their digital identities and grant governments and companies permissions to access, rather than the other way around. The BBC recently investigated the story for *The Today* programme:

*I've just acquired a whole new identity. It comes in the form of a plastic card with a chip in it, and it means that I am now a resident of Estonia. Or rather an e-resident, because this card is a symbol of Estonia's bold ambition – to export its expertise in digital identity to the wider world.*

*The e-Residency programme, which has already attracted 10,000 people from around the world, offers anyone who pays 100 Euros some of the benefits of the digital ID cards which Estonia's 1.3 million citizens have had for more than a decade.*

*I meet Kaspar Korjus, the young manager of this project, at the e-Estonia showroom in Tallinn, where the government shows foreign visitors the progress it has made down the road to digital public services. Kaspar*

*starts by showing me his own digital ID – he's 38712012796 by the way, though that won't be useful to you without his card and two PIN numbers.*

*We go online to a site where he can check which data is held, linked to his ID – his doctor, his driving licence, his family circumstances. He explains that he has control over that data and it could not be shared without his agreement. His ID card is even used for voting – “I've been travelling quite a lot – the last four times I was away but I could still vote. I use PIN 1 to confirm who I am, PIN 2 to vote.”*

*While e-residency will not allow me to vote, or permit someone from outside the EU to travel here without a visa, it does confer a number of advantages. It makes it a lot easier to set up a business and open a bank account, and you can use the card to digitally sign documents and contracts.*

*This is a country which does not worry about immigration – indeed it would like more people to move here. Kaspar tells me they are put off by the weather and the remoteness of Estonia but the hope is that e-residents will boost the economy by starting businesses here without needing to move.*

*He quotes one example – Stanislaw, a painter from Ukraine, who was unable to sell his pictures because his country does not have the infrastructure to allow him to accept foreign payments. “PayPal will work with someone who has a business address in Estonia,” says Kaspar, “but not with someone in Kiev.” Now the artist has established a company in Estonia and is selling his paintings around the world while remaining in Kiev.*

*One obvious thought strikes me about the e-Residency program – isn't it all about avoiding tax? “It's actually the complete opposite,” says Kaspar Korjus. “Every transaction is recorded, your identity is there, it's all very transparent.” The expectation is that just about all e-residents will pay tax on any earnings where they are generated – in their home countries – and the Estonian government will transmit details of revenues back to local tax authorities.*

*Estonia hopes to benefit because of the business generated for its banking and advisory services, rather than in direct revenues. Then there is the interesting prospect of linking this digital identity service to the blockchain, the technology underlying the virtual currency Bitcoin.*

*One such experiment is already underway. NASDAQ, which runs the Tallinn stock exchange, is creating an e-voting scheme, allowing shareholders to vote at annual general meetings. The e-Residency platform will be used to identify voters, while the blockchain will provide a fast and secure way of recording the votes.*

*The e-Residency project is very much a work in progress. While it's of limited use to me at the moment, I can see my new digital identity becoming a way to authenticate myself on e-commerce sites and other places which want to know you are who you say you are.*

*Kaspar Korjus is convinced that this is an idea whose time has come, and countries will compete to offer this kind of virtual citizenship: "We are the first mover – there will be lots of e-Residency programmes." He has been set a target of attracting 10 million e-Estonians by 2025. That sounds ridiculously ambitious, but this tiny country has already shown that, when it comes to being digital, it can punch far above its weight.*

It's an amazing program and one to watch. The key is that citizens should own their data and manage their identities. Why should I give my identity to a centralised structure that could be compromised? That is the whole reason why there are so many issues with identity today, because centralised organisations get hacked and our details are stolen. I want to control my own identity. That is the key, and it is coming as Estonia has shown.

This has led to other projects. There's the United Nations Digital Identity program that I blogged about recently and, importantly, the World Economic Forum recently issued a report focused upon *Disruptive innovation in financial services: A blueprint for digital identity*.

*The report calls on financial institutions to lead the charge in developing robust digital identity solutions that would bring benefits to users, financial institutions, and society as a whole. Some of the critical steps outlined in the report include studying and understanding the user group, engaging with the public sector, and determining the technology backbone needed for the identity system. While not intended as a roadmap, this report will serve as a foundation for entities wishing to understand and ultimately act on the identity challenge.*

The mandate of this project was to explore digital identity and understand the role that Financial Institutions should play in building a global standard for digital identity. The 108-page report proves of interest and I thought I would copy a few of the key pages here:

They then outline the different schemes that are in play:

Their solution is basically a mixture of decentralised identity structures with some centralised oversight: “The centralized and distributed identity archetypes would solve many of the business challenges that FIs are currently experiencing.”

But, when it comes to digital identity, I often defer to David Birch as he’s written a book on the subject, as well as blogging about it regularly since I was an embryo.

In his latest blog, he talks about the World Economic Forum's report:

*The report suggests three approaches, which I paraphrase here:*

- A single **institution** could create its own system, focusing on cost saving but with limited potential for further adoption (but I think "ChaseID" would struggle against "AppleID");
- A **consortium** could create a co-opetition infrastructure along the lines of the payment networks (some sort of financial services passport);
- The financial services sector as a whole could create some form of **industry** identity utility that could be used to deliver "wholesale" identity services (I could get gas, electricity and identity all from the same retailer);

*I'm rather in favour of the middle option as I think it delivers immediate improvements to the day-to-day transactions of modern life and it is, above all, feasible. But what exactly would it implement?*

*The model of identity transactions that the WEF present (page 43), which divides identity transactions into authorisation, attributes and authentication is I think a little too narrow.*

*The model we use at Consult Hyperion ("Three Domain Identity", or 3DID) provides a better platform for discussion and exploration (but then I would say that wouldn't I) because it makes the relationships between identities, attributes, credentials and so on more explicit.*

*When it comes to discussing archetypes (or “marketectures”) that will make sense (page 62), the use of the 3DID model makes it easier to understand the different options but considering who will control each of the domains. If, as WEF recommend, it is the financial institutions who control the Digital Identity and they link this to a variety of Mundane Identities from different sources as well as to a potentially large numbers of Virtual Identities (where credentials are held, essentially) it gives them a pivotal role. This might be in a federated structure, where each banks holds its own KYC and makes it available to other banks, or some other options. However it’s done, the authentication (proving you control the digital identity) is another matter ...*

*In conclusion, despite my preference for our model, when it comes down to it, I think that the middle way (the consortium approach) is the place to start and I strongly agree with the principal recommendation of the report, which is that (page 101) “Implementation of a digital identity system should follow a bottom-up approach”.*

And what’s this got to do with blockchain?

Well, as outlined, blockchain is not the solution for digital identity. It’s a database technology that can potentially help but the challenge is the identity scheme structure, as discussed, rather than the technology being used to solve it. Adam Cooper is the lead technical architect for the Identity Assurance Programme within the UK Government’s Digital Service, part of the UK Cabinet Office, and he wrote an insightful blog about the subject:

### **Does digital identity need blockchain technology?**

*The consensus of identity experts seems to be a resounding no. You can build distributed ledgers without resorting to the blockchain, and you can preserve privacy in many other ways. Identity can be improved but it simply isn’t broken, so it’s hard to see where blockchain technologies are really required.*

*There are potential uses for blockchain type technologies in the creation of immutable evidence chains for individuals wishing to prove their identity. For example, where the individual is starting with no or minimal evidence and needs to build a chain of evidence over time, as is the case for refugees. There may also be applications for personal data stores and attribute services associated with, or unlocked by, verified identity that can enhance the ecosystem.*

*There are some basic maturity issues with these technologies including the lack of standards, common*

*terminology, or demonstrable examples of 'real' implementations. Some of this is to be expected at this stage but, where there are known scalability and security issues left unanswered, the risk of implementation may outweigh any benefit. Blockchain is unproven.*

*The other problem with blockchain technologies is that the clock is ticking. We are yet to see tangible results that make blockchain a mainstream product. Already, alternative technologies are emerging. Swirlds, for example, utilises a hashgraph data structure and the Swirlds consensus algorithm to create a platform for distributed consensus much the same as that claimed by blockchain.*

So Adam feels we don't need blockchain to solve the identity problem. What does the WEF report say:

And what does David Birch think?

Well, you can find out by spending half an hour watching his fantastic presentation about identity and blockchain from Vince Everts' Dutch Blockchain Conference in June.

David Birch - How to use Identity & the Blockchain | Dutch Blockchain Conference #dbc16





In this presentation, David makes a number of key points. For instance, he proposes that you have many identities. Some are used for banking, some for visiting schools, some for going to football matches and so on and so forth. We have those today: bank cards, loyalty cards, library cards, university cards. All of these are different virtual identities linked to your core identity: you.

David's model is that your core digital identity is you, and that is managed under a shared ledger which, if you remember, is more than just a blockchain. The shared ledger comprises blockchain, a digital currency, digital signatures and a consensus mechanism. You can then create a number of other identities – pseudonyms – that are authorised by your core digital identity to transact on your behalf. These he calls virtual and mundane identities. As a result, you end up with many virtual identities linked to many mundane identities, with a digital identity in the middle as the controller. Otherwise you would have many-to-many identity schemes that would fail, as a basic of systems analysis is that structures need to be based upon one-to-many schemes (one digital identity to many virtual and mundane identities). That's the illustration that Dave gives in the chart I shared earlier.

In David's view, blockchain as a component is worthwhile for verifying virtual identities, but not for storing digital identities. He states that you need to have a private digital identity that you control, that is not on the blockchain, but on a shared ledger. That identity can then authorise the creation and usage of your public virtual and mundane identities, which are on the blockchain. For example, a bank can verify my existence through a check on my virtual identity from a previous bank. Knowing that a previous bank opened an account for me is enough to verify that I am good to open an account with them. Their check is with my bank virtual identity which is on a blockchain, but my core digital identity has not been accessed.

It is for this reason that Mr. Birch attacks anyone who talks about blockchain for digital identity when they mean shared ledger, as the two are distinctly different. I doff my cap there and conclude that both Adam Cooper and David Birch are correct – there is a difference between blockchain and shared ledger, and

tomorrow I'll look at the companies that are using both to create our next generation of digital identities.

---