The Future of Personal Identity

The opportunities and risks for banks within the emerging identity marketplace

2019

Finextra

Expert Contributors:

SIGNICAT
HID
OneSpan
The Future of Personal Identity: The opportunities and risks for banks within the emerging identity marketplace

Introduction

Chapter 1: Personal identity hype
Expert view: Christine Leong, Management Director, Blockchain, Identity and Biometrics, Accenture

Chapter 2: Big player power
Expert view: John Erik Setsaas, VP Identity and Innovation, Signicat

Chapter 3: Fake data and trusting vulnerability
Expert view: Ali Babakhan and Daan Van Den Eshof, Product Managers for Rabo eBusiness, Rabobank

Chapter 4: The binary opposition of CX and free data
Expert view: Olivier Thirion de Briel, Global Director FSI Market with IAM Business Unit, HID Global

Chapter 5: Biometric and blockchain experimentation
Expert view: Frederik Mennes, Senior Manager, Market and Security Strategy, Security Competence Centre, OneSpan

Conclusion
Bibliography
About Finextra
2018 saw the implementation of the General Data Protection Regulation (GDPR) across the European Union and European Economic Area and subsequently in the UK, a new version of the Data Protection Act (DPA) was enacted. Despite this new wave of regulation, lack of security in new technology may call for yet more standards in the future.

Technology providers, financial institutions and governments are all being closely scrutinised following a year of substantial data breaches and compromises of trust. Most notably the Cambridge Analytica and Facebook scandal, has resulted in the marketplaces in the US and UK looking to learn about best practices and innovation from other countries.

This report on The Future of Personal Identity analyses the advantages and disadvantages of private, public and federated identification systems and whether industry leaders believe that banks are in the best position to provide trusted authentication services.

With data underpinning every aspect of today’s society, banks are now using the importance of protecting their customer’s personal identity as a catalyst to digitise products and better compete with new players that may be less secure. In response to increased public awareness about the rights individuals have over their personal data, financial institutions are reinventing their businesses and strategies to rebuild trust and position themselves against Big Tech as the champions of data equality.
As we progress further into 2019, it is evident that the issues and opportunities surrounding the topic of identity within the financial services marketplace are undergoing fundamental change. Because of technological advance, digital verification is playing a larger part in banking.

Developments such as social media and mobile phones have provided many more people around the world with access to financial services. As a result, new ways of validating and verifying existing and potential customers have come to the fore but significant problems arise when these systems are compromised, raising new challenges for banks.

While the World Bank’s ‘Global ID4D’ Dataset estimates that there are currently one billion people who cannot prove who they are, the emergence of digital authentication has also provided many sectors of the population, especially those who struggled beforehand because of socioeconomic factors, with increased access to public and private services such as healthcare and education.

This digital new normal has led to an expansion of the identity industry. Governments, regulators, companies and banks across the globe are now attempting to manage both personal authentication and the associated data security and policy questions arising.

Despite this acceleration in available technologies, traditional banks continue to ask their customers for identification such as birth certificates and passports when opening a new account at a branch. They do so despite the economic advantages of moving to new identity services. According to the Boston Consulting Group’s report ‘The Value of our Digital Identity’, the adoption of digital identity services could lead to a significant annual value growth of 22%, which would result in €330 billion by 2020 for the private and public institutions in Europe.

Reluctance

In the UK, at the start of 2019, governor of the Bank of England Mark Carney suggested that digital ID cards “would make it safer for people to access money online” and that improvements need to be made to the security and privacy of online financial services, not only to customer experience, as reported in The Telegraph. Following the internet boom and the parallel decline of bank branches, this harmonisation of different systems of online identity verification is overdue. As cybersecurity increases as a major concern and digital criminals improve their capabilities to threaten both individuals and the wider financial system, the imperative only increases.

National culture and historical legacy have played a key role in approaches to identity issues around the world. In the UK, the concept of an ID card has always been a controversial subject despite almost every other European nation using one. Back in 2010, the UK’s Coalition Government scrapped a plan inherited from its predecessor to introduce identification cards. The then home-secretary, Theresa May, said that the scheme would increase control over citizens. A year later, the Cabinet Office started work on the GOV.UK Verify system. It was declared live on 24th May 2016.

In March 2019, GOV.UK Verify was criticised in a National Audit Office (NAO) report after only 3.6 million users had signed up for the digital identification scheme – way off the 2020 goal of 25 million. The NAO report examined the Government Digital Service’s (GDS) expectation that the flagship identity verification platform would cost £212 million and generate £873 million between 2016 to 2020. The UK Government, however, claimed that drawbacks like this were normal when introducing new technology, despite the initiative’s intention of becoming the default identity verification process for online services such as benefits or income tax.

At the latter end of 2018, the minister responsible for implementation, Oliver Dowden CBE MP, made a House of Commons statement that highlighted that the UK’s GOV.UK Verify programme was ready to enter the next phase of development. GOV.UK Verify promotes itself as a secure way of proving who you are online and one way that a UK citizen can access government services such as taxes or their driving license. The UK Government has partnered with Barclays bank, identity provider Digiidentity, credit reporting agency Experian, the Post Office and verification service SecureIDentity to offer this service. Consequently, all these private sector organisations are certified to verify identity on behalf of the UK government.

In his statement, Dowden said that now the government digital service was mature, the "private sector will take responsibility for broadening the usage and application of digital identity in the UK." While the government will continue to provide assurance, the UK’s identity scheme operates under commercial organisations. Success in the marketplace will be determined this way, without direct funding and investment from the government. The announcement also ensured "that GOV.U.K Verify will continue to protect public sector digital services from cyber threats, including identity fraud, and other malicious activity."

"the World Bank’s ‘Global ID4D Dataset’ estimates that there are currently one billion people who cannot prove who they are"

However, in conversation with Finextra Research, head of thematic research and chief analyst at GlobalData, Gary Barnett, says he believes that "while the Verify programme does purport to be useful beyond providing identity assurance for public sector services, there’s been next to no uptake. This is partly because organisations like banks or insurance companies already have established identity assurance and know your customer (KYC) processes in place – many of which are not all that compatible with GOV.U.K Verify."

People deal with digital platforms that are not customer-efficient in three stages: irritation, dejection and then, acceptance. Consumers understand that problems arise and may take time to resolve. What we are seeing in the UK is that the Government would like the private sector to lead and refine how identity services are provided to the public.

On the other side

Agility is necessary in identity services and a simple way of providing this would be to establish just one process of authenticating citizens. In the US, the Department of Treasury released a report emphasising the importance of portable digital identity: the report pointed to the significance of establishing legal identity for new customer relationships at financial institutions without the need for the bank having to verify personally identifiable information (PII).

This proposed US plan has strong parallels to the UK’s groundbreaking Open Banking experiment and in the same way, stated that "trustworthy portable third-party identity services could potentially save relying parties time and resources in identifying, verifying, and managing customer identities, including for account opening and access."

The US Treasury also put forward a request for financial regulators to collaborate with them so that unnecessary barriers which private and public organisations might face could be eliminated, and the adoption of digital identity services would be better facilitated within the financial services industry.

Speaking with Finextra Research, Alex Bolante, managing director, consumer identity management at Deloitte Risk and Financial Advisory, discussed the US situation. Bolante considers that US financial institutions were already aware of the need for and benefits of digital identity. However, as customer expectations rise, so do those of the regulators.

According to Bolante, "regulators are demanding increased transparency around transactions, meaning that financial institutions require greater granularity and accuracy in the identity information that they capture and are increasingly being held liable for inaccurate or missing identity information."

He adds that "bad actors in financial systems are increasingly sophisticated in the technology and tools that they use to conduct illicit activity, increasing their ability to quickly cause financial and reputational damage by exploiting weak identity systems."

Identity risk

Despite this risk, banks could stand to benefit from creating digital identity solutions. Money and identity are two closely intertwined concepts that have started to operate on a parallel basis. In conversation with Finextra Research, Kaelyn Lowmaster, head of research at One World Identity, highlights that "those two goals – financial institution success and personal identity protection – are not necessarily in conflict with one another. It’s in the best interest of a financial institution to make sure that consumer identity is protected to avoid theft, fraud and compliance violations."

The contrast between banks and Big Tech – an alternative source of consumer identity services – is stark in this regard. Lowmaster continues: "reliable identity data is critical for accurate risk assessment, financial product underwriting, and marketing – but we find it’s helpful to think of personal data protection as a potential strategic differentiator for financial institutions."

On data protection – a significant talking point in 2018 and not just in the financial services industry – digital bank Tandem’s chief technology officer Paul Clark reiterates to Finextra Research there will always be a new threat for banks, and therefore they have a responsibility to inform and educate their customers.

"The truth is that good service is built on a wealth of data and that benefits the customer and the bank. Part of data protection is keeping consumers aware. If you aren’t using customer attention to improve their security, you are doing something wrong," Clark says.
Expert view:
Christine Leong
Managing Director, Blockchain, Identity and Biometrics
Accenture

In an interview with Finextra Research, Christine Leong, managing director, blockchain, identity and biometrics for Accenture highlights that the recent interest in identity and security of personal data has been “a long time coming.”

Christine Leong advises that there is an increasing need to be trusted and validated as the world becomes increasingly digitised and governments and financial institutions alike need to ensure that the person they are authenticating is who they say they are.

She went on to reference a recent World Economic Forum report, ‘Identity in a Digital World: A new chapter in the social contract’, that focused on the importance of establishing trust in a digital economy.

The report stated: “All over the world, a growing number of organizations – from the public and private sectors – are advancing systems that establish and verify digital identities for people, devices and other entities. This community is expanding in scope, growing beyond traditional identity practitioners to include a broader set of actors exploring the promise and perils of digital identities – from domains such as healthcare, financial services, humanitarian responses and more.

“Yet we are still learning what ‘identity in a digital world’ means. We are also still evolving policies and practices on how best to collect, process or use identity-related data in ways that empower individuals without infringing on their freedoms or causing them harm. There is significant room to improve how identity data is handled online, and how much control individuals have in the process.”

Leong also points out that whenever national identity is discussed, culture is a factor. Different countries have different cultures, and this can play a major part in how and to what extent governments get involved. “Governments are having discussions about whether a national ID is a good idea but while in most countries governments are trusted entities, this is not the case in all.”

Leong continues: “The UK and the US are arguably two of the most influential countries in the world and while most people in both countries use driving licenses as a form of ID, I think initiatives like GOV.UK are forward-thinking. There is a need for the public and private sector to work together to establish trust and ensure that identity proving is completed to different levels of assurance. This is going to become more and more important, while the UK and the US are already looking at these initiatives, there are still more coming.”

She expands on the collaboration of the public and private sector, stating that “banks have a huge role to play in countries in which they are more trusted than governments. Private institutions are more trusted, partly because governments change, but also most people residing in developed economies already have bank accounts. Alongside this it is important to remember that few change their bank over their lifetime whereas governments come and go. Banks have a huge role to play in terms of establishing trust, helping to provide verifiable credentials for us to transact with, and to establish ourselves as a trusted entity in the digital world.”

While financial institutions are still working on their customer experience initiatives, Leong suggests that more should be done in terms of Know Your Customer (KYC) and ensure that the appropriate measures are taken in terms of compliance with GDPR and other new regulatory data protection requirements.

In addition, Leong believes that there is an emerging trend for decentralised identity. Inevitably blockchain and distributed ledger technology (DLT) are factors. Blockchain adoption could – theoretically – allow users to control their own data and manage their personal information over time, for example, manage mobile phone contracts and prescriptions in the same place.

“Blockchain will enable this but I do think that there is some way to go in terms of understanding what the technology can do. The user experience aspect is also critically important for identity services, centralised or decentralised.” New services need to ensure that the underserved are also given a voice and the ability to be verified, which could be provided with biometric offerings.

As Leong explains, ‘passwords are very old technology.’

While biometrics is accepted in some cultures, the technology is not in other countries. The iPhone pioneered the opportunity for biometrics to enter the mainstream. Aside from reducing friction, biometrics can be effective for those who cannot write or sign.

Similarly, biometrics cannot easily be lost or stolen. Leong concludes by discussing the Indian government’s decision to issue an easily verifiable 12-digit random number to all residents of the subcontinent in 2009. She adds that despite the data breach and additional software hack that allowed unauthorized persons, anywhere in the world, to generate Aadhar numbers in 2018, uptake by 1.2 billion people cannot be ignored.
Big Player Power

In 2015, the United Nations set out to achieve 17 Sustainable Development Goals⁶ to address the global challenges that the world faces in relation to poverty, climate and environmental degradation, among other things.

Alongside aims such as zero hunger, gender equality and clean energy, Goal 16 of 17 titled Peace, Justice and Strong Institutions, promised to provide a legal identity for all, including birth registration by the year 2030.

The implementation of worldwide birth registration is an important step. It protects individual rights and helps to give control of personal identity back to the citizen. While physical forms of identification, such as passports, have always been issued by governments, it is evident that this would not be the best form of authentication for those potentially under threat or at risk. Central to this argument is whether governments should be digital identity providers, or if a private or even a federated identity system would offer increased security for the citizen.

At the start of this year, the Emerging Payments Association (EPA) advised UK financial institutions and payment processors to collaborate on creating a national digital identity scheme to prevent the threat that is posed by money laundering and payments-related financial crime.⁷ In a report put together with support from a group of EPA members including Refinitiv and Barclays, recommendations were set out for industry members on how to tackle the threat of fraudsters and money launderers’ abuse of payment services and bank accounts.

Speaking with Finextra Research, James Mirfin, global head of digital identity and financial crime at Refinitiv, refers to governments as the “ultimate issue authority or ‘golden source’ of identity.” For many around the globe, a public ID card that operates both physically and digitally has been beneficial.

The Albanian case study


Because of the ‘Digital Albania’ initiative, 3.2 million smartcards and 2.6 million biometric e-passports were issued by Albania’s Ministry of Interior Affairs, an Albanian subsidy of identity solution provider Morpho, now known as IDEMIA, and non-profit Albanian-American Enterprise Fund (AAEF).

Once citizen data is validated against a central database, Albanians have the capability of obtaining passports within 24 hours of less for an extra cost and after an agreement was reached with the European Commission in 2010, Albanians have the right to travel throughout the Schengen area without a visa.

As revealed in BBVA Research’s Working Paper “Digital Identity: the current state of affairs,”⁹ 82% of all countries providing national ID Cards had rolled out eID, or electronic ID, programmes by early 2017. In addition to this, 55% have access to digital identification for services such as health or voting, but only 3% can use an ID scheme that operates both online and offline. Also, 24% of developing countries have no form of established digital identity service whatsoever.

BBVA highlighted that the best example of federated identity is the use of government issued IDs for a range of different private services. “Public and private sector firms have a mutual interest in developing digital identity systems that allow the identification and authentication of users for different functions and services. Moreover, both public and private incumbents may rely on each other to build and manage identity schemes.”¹⁰

The report continued: “Collaboration models can be different depending on the type of the project and the scope of private sector involvement. Sometimes, private providers act proactively to use public IDs. In other instances, public authorities ask the service provider to rely on its ID.”

---

⁷ Finextra, ‘Payments body calls for digital IDs to tackle financial crime’ (2019).
James Mirfin, global head of digital identity and financial crime at Refinitiv, refers to governments as the “ultimate issue authority or ‘golden source’ of identity.”

In addition to this, Mirfin reveals to Finextra Research that governments should “focus on open federated digital identity platforms which provide inter-operability and enable non-governmental services. This can help drive citizen adoption and private sector usage. However, there are too many examples of government programmes which are sub-scale, and they tend to focus too heavily on low velocity citizen services as the primary driver of adoption.

A cautionary tale

An example of a federated identity system could be the UK’s GOV.UK Verify framework. However, there has not been a positive response to this scheme, as Kaelyn Lowmaster, head of research at One World Identity, points out. She says that it has “turned into a bit of a cautionary tale”. Lowmaster adds that “it didn’t hit its enrolment targets, user experience was poor, and the government has pulled funding from the project. But overall, good digital identity at the national level has an enormous amount of potential to improve both governance and quality of life.”

She also explains that the US’ Social Security Number (SSN) could be considered a counterpoint to the UK experience. In the US the SSN, “was never intended to be a national identifier but has become our default identity system. Both overuse of SSNs and data breaches have exposed some real security issues with this ad hoc system. The conversation on what should replace the SSN is once again coming to the fore in the US.”

The Indian case study

The Unique Identification Authority of India (UIDAI) relied on third parties, such as state governments, banks, telecom companies and insurance agencies to collect data, to reduce cost and inefficiency. The World Bank and GSMA reported that over one billion people have been registered and in addition to biographical information, fingerprints and iris scan data was encrypted and stored.

However, what has been dubbed as the world’s largest biometric ID system, has been subjected to a multitude of hacks, notably in 2018 when hackers changed enrolment software code in 26 places, as reported by The Huffington Post. 10

Last year, an inexpensive and malicious software patch was sold over WhatsApp and allowed users to bypass biometric authentication and would disable the built-in GPS security feature, allowing anyone anywhere in the world to be able to enroll users.

The security patch also reduced sensitivity of the iris-recognition system, making it easier to spoof software with a photograph rather than requiring the operator to be present in person. Activity such as this suggests that advice given by EPA could prove to be beneficial across the world. Collaboration between banks and national digital identity schemes could prevent the threat of data breaches, because of KYC processes already in place.

The example that Accenture’s Christine Leong provided could be considered here. As detailed in the World Bank and GSMA report, the Indian government embarked on the ambitious task of enrolling 1.2 billion people to a digital identity system in 2009. The meant that every citizen would receive Aadhar, a unique number that would serve as proof of identity.

In a Q&A interview with Signicat, John Erik Setsaas, VP identity and innovation, outlines whether there is a demand for digital identity management solutions, who is in the best position to offer these products and what needs to change in the onboarding process.

**Expert view:**

John Erik Setsaas
VP Identity and Innovation

**www.signicat.com**

Yes, absolutely. Service providers spend a lot of effort on onboarding, and based on our research, still lose more than 50% of their potential clients. An electronic identity, which has been proven by some trusted entity, will help in this process. The user will not have to provide the same information repeatedly, while the service provider will receive information they can trust.

In Norway, there is a 93% penetration of BankID with the adult population, and on average, each Norwegian uses BankID three times per week. Despite the name, this is not limited to banks. It was initiated by the banks in 2005, but the success factor was when this was extended to also be used for filing taxes. And since then it has grown and being used for more services. Today, I can use BankID to login to banks, insurance, government, health. It can also be used for onboarding, and to become verified buyer/seller on person-to-person trading platforms, and even for age verification for tanning salons.

Banks have two very important elements that are crucial to the success of digital identities: consumer trust and frequency of use. Consumers log into their banks regularly, when compared to government identities. However, the field of identity is complex, and fintechs/technology providers who are specialised in identity will be able to assist in this. A good example of this is the cooperation between Signicat and Rabobank. Rabobank is a known and trusted brand in society, while Signicat has been working with the challenges of identity for more than 10 years. In addition, the government must be a user of the identity scheme, by letting the users file their taxes, start a company and perform other government related functions using their eID. The government also defines the regulations on how eIDs can and should be used, and as such plays an important part of the identity puzzle.

Where have you seen digital identity work?

In Norway, there is a 93% penetration of BankID with the adult population, and on average, each Norwegian uses BankID three times per week. Despite the name, this is not limited to banks. It was initiated by the banks in 2005, but the success factor was when this was extended to also be used for filing taxes. And since then it has grown and being used for more services. Today, I can use BankID to login to banks, insurance, government, health. It can also be used for onboarding, and to become verified buyer/seller on person-to-person trading platforms, and even for age verification for tanning salons.

Who is in the best position to offer digital identity solutions?

Banks have two very important elements that are crucial to the success of digital identities: consumer trust and frequency of use. Consumers log into their banks regularly, when compared to government identities. However, the field of identity is complex, and fintechs/technology providers who are specialised in identity will be able to assist in this. A good example of this is the cooperation between Signicat and Rabobank. Rabobank is a known and trusted brand in society, while Signicat has been working with the challenges of identity for more than 10 years. In addition, the government must be a user of the identity scheme, by letting the users file their taxes, start a company and perform other government related functions using their eID. The government also defines the regulations on how eIDs can and should be used, and as such plays an important part of the identity puzzle.

Are regulations in place enough for banks to do due diligence on their customers?

Banks are under the AML (Anti Money Laundering) regulation, and as such have an obligation to determine the identity of the users, to prevent money laundering and terrorist financing. The regulation does not define how this is to be done. The new eIDAS regulation has an implementing act which gives some indication as to what is required to assure a user on the highest level (eIDAS defines: “Low”, “Substantial” and “High”), which should be enough to fulfill the AML regulation. However, there are checks which is outside determining the identity of the user. Even though you can verify a user on High level, they may still be doing illegal activities. The banks must also check things like PEP (Politically Exposed Person) lists, credit ratings, and obtain other economic behavioural data as part of the due diligence. Again, there is no regulation defining how this should be done.
Signicat operates in multiple markets and countries and our focus is to create a platform where each customer can combine identity assurance methods to satisfy their requirements as put by the regulators. We are constantly looking for new and better ways to ensure the users’ identity. It is important to note that the KYC process continues by the bank after the onboarding process is done. The bank will monitor the usage patterns, to get to know the customer even better.

SCA is a must for secure services today. People are too sloppy with passwords, including reusing the bank password on unsecure sites. SCA ensures that an attack on an unsecure site does not automatically give access to a bank. The second factor does of course add extra friction for the user, which is why Signicat is exploring the possibility to use adaptive authentication, where user behaviour can be included in the authentication process. To put it simply, the mobile device knows whether it is in the user’s possession, based on location, available networks, how the user walks etc. This combined with risk evaluation could determine whether an additional factor is also needed.

As has been proven time and again with cryptocurrencies, when you lose your private key, there is no recovery mechanism. We, the identity community, have already put enough responsibility on the users to remember passwords, which most people do not understand or manage well. We cannot put even more responsibility on them, by requiring them to be their own identity provider. We need to depend on trusted entities, like banks, to be identity custodians, and do this work on behalf of the users.

The most important thing that has happened for privacy is GDPR, which focuses on the user data. We have all been overflown with consent e-mails and pop-ups, which is a nuisance, and will have to be improved, by putting the user in the center of this. But GDPR shows that it expects the organisations to manage identity data properly, by putting very high fines in breaches. From a privacy perspective, this will discourage most organisations from collecting more data than they need and by using an eID, you will need to collect even less, as this is handled by somebody else. GDPR has changed user data collection from an asset to a liability.

Has the Know Your Customer regulation changed how you operate?

How do you benefit from being offered Strong Customer Authentication (SCA) by banks?

How has GDPR affected the new frontier of privacy we are entering?

Do you have concerns about blockchain being used for identity services?
Some of the biggest victims of last year include Google, T-Mobile, Quora and Orbitz, but the most notable for the financial technology industry was perhaps the British Airways hack, that affected card payments made via the airline’s website and app in August and September 2018 by some 380,000 customers.

As already referenced, 2018 also marked the year that GDPR was implemented. The regulation ensured that both physical and digital identity management solutions enforced the idea of the individual’s control over one’s own data, with the most important provisions being the right to access, right to be forgotten, right to portability and right to data minimisation.

Unfortunately, GDPR has failed to deter those with criminal intent. Hackers continue to find new ways to attack, which means that security will need to improve to ensure that data theft, password loss, token compromise, illicit communications surveillance and phishing does not occur.

Tackling vulnerability

In conversation with Jean-Michel Garcia-Alvarez, head of internal audit and data protection officer at OakNorth, he highlights to Finextra Research that banks would be best placed to help reduce worry about increased vulnerability, “by continuously improving the security around the personal data they process and by having plans in place to effectively support customers once a data breach occurs.

"For instance, a recent breach at a national airline provided a very poor customer experience (we had a breach, please talk to someone else – your credit card provider – about it) that fell short of everyone’s expectations and increased worry, not reduced it.

"In contrast, a major credit card issuer sent an email to all its customers saying they were aware of the breach at the airline and their fraud systems were monitoring the situation closely and that card holders had nothing to do and were protected. Communicating with, and effectively supporting, customers is what needs to be done." This credit card issuer was able to turn a moment of anxiety into an opportunity to build confidence.

The question arises, whose responsibility is it to inform the customer, and following this should governments produce a form of identification or should banks have a process in place to ensure data protection?

The data breach that threatened Aadhar last year hit India’s national ID database and affected every one of the 1.2 billion participants that were subscribed to the authentication database. This highlights the more significant target offered, scaled, national solutions are still at risk.

BBVA referenced World Bank research in their report and revealed that 50% of countries with a national identity card system do not have data protection legislation in place. This escalates as an issue when a person’s information must be collected, stored and shared in a safe and appropriate manner.

The World Bank report in collaboration with mobile network operator trade body GSMA echoed this consideration: "Countries that choose to adopt digital identity systems must have robust legal and technical frameworks for data protection and privacy.

“Missteps in handling citizen data can erode trust in government and decrease the value of the system, threatening revenues and the efficiency gains derived from personal data applications.” The report then went on to reference a study that estimated that in 2020 alone, two-thirds or $480 billion, of the potential value of digital ID in the European Union would be at risk if personal data is not secure.
Should banks create a digital ID?

Deloitte’s Alex Bolante believes that “there is a strong business case for financial institutions to lead the development of digital identity systems, not only to mitigate risk but also provide other benefits to users.” Bolante identifies the following reasons why banks should offer authentication solutions.

Privacy and control
- Users would have full control over which Identity Providers (IdPs) hold their attributes
- Users’ consent would be required before IdPs could expose attributes
- User data would not be sold by third parties
- The minimum amount of user information required would be transferred during transactions

Security
- User attributes would only be held by entities meeting system standards and requirements for information handling and storage
- Digital attribute storage would make identity information resistant to damage, destruction or loss
- Users would have the ability to disperse their identity information, creating contingency if an IdP suffered a data breach or data were erased or stolen, and reducing the impact of a data breach on the user

Convenience
- Digital identity and digital attribute transfer would simplify and improve the user experience in transactions, eliminating the need for users to track multiple authentication methods (e.g., usernames and passwords) and manually submit personal information during transactions
- Attributes would be transferred digitally, removing the potential for human error and subsequent information remediation
- Users would be able to easily update information held with their IdPs and would not have to deal with transactions being executed based on inaccurate or out-of-date information

Transparency
- Users would have visibility into which attributes would be exposed and to what entity during identity transactions

Bolante adds: “Financial institutions are exceptionally well positioned to build digital identity systems that fill the gaps left by current efforts.” Banks already act as stores of customer data for commercial purpose, can verify user information, collect accurate user information and develop new systems and standards, so creating a digital identification should not be a problem.

In addition to this, Bolante says that financial services have near-complete coverage of users in developed economies, whether people, legal entities or assets, and because global banks have operations across a number of jurisdictions, they have an advantage in enabling identity transactions and systems across these areas.

The question arises, whose responsibility is it to inform the customer, and following this should governments produce a form of identification or should banks have a process in place to ensure data protection?

Revenue growth
- IdPs would complete identity transactions for RPs; this would allow them to monetise identity-as-a-service through per-transaction fees or other business models

Defined risk and liability
- Liability guidelines would be clearly defined and communicated; IdPs would be clear about their liability in the event of data loss or breach, or contravention of the standards for identity provision

Competitive positioning
- IdPs would be able to forge a strong relationship with users and position themselves as a critical part of the digital economy, given their unique insight into users and their established position of trust

Improved products and services
- IdPs would have increased access to detailed and reliable user information that would allow them to better tailor processes, products and services
- IdPs could begin to draw on non-standard user attributes to better manage and evaluate risk (e.g., health records)
- Secure digital identity protocols and digital attribute transfer would improve user experience and expand the number of services that IdPs could securely provide online

Bolante concludes that we are increasingly “seeing FIs talk more about how they’re trying to earn customer trust. However, they need to go further and create ‘trusted experiences.’”
Babakhan and Van Den Eshof highlight that after leveraging this experience in online payments, Rabobank were able to transfer what they had learnt in this area to a new market space for Rabobank: e-Identity and value-added services that go with it. With help from their Norwegian partner Signicat they gathered knowledge from the Nordics to apply to the Dutch market. They referenced Norway’s national ID card scheme, which has garnered media attention for the staggering $86 million cost it will require to issue new national ID cards to all residents.

Van Den Eshof says that “while a government-issued ID seems like the logical option, tech companies, banks and telcos all have a great reach to end users in the market and input from multiple entities could also be beneficial.”

In fact, Finland was the first country to roll out a national electronic identity card, which the Nordic state did in 1999 according to the World Bank and GSMA report. Since then, multiple forms of identification have entered the marketplace, but the banking sector ensured that two-factor authentication involving a unique ID number, a PIN code and one-time password was part of the process.

The report revealed: “In 2008, in response to challenges of impracticality and underuse the existing systems were facing, a consortium of government agencies, mobile operators, and the Finnish Federation for Communication and Teleinformatics (FiCom) agreed to launch a mobile identification system that would combine the benefits of the existing systems and be more accessible to the public.”

Van Den Eshof took the discussion outside of the Nordic region and spoke about the Dutch bank-ID, called IDIN, which was introduced in 2016 by the Dutch banks as a substitute for the government e-ID. In 2018 followed by Belgium’s national ID card, which has two signatures: one for authentication and another for electronic signature.

He likens the way that the Belgian government has worked with banks and mobile phone service providers to provide identity solutions to how electronic payments gained mainstream use. However, he adds that while governments are in the best place to provide IDs because of regulatory restraints, banks and telcos are more experienced in providing efficient customer experience.

Speaking of mobile solutions, Estonia’s mobile identity solution m-ID has been heralded as a model case – the Government of Estonia having offered electronic services through its eGovernance initiative since the 2000s.

In 2007, a mobile operator began offering mobile authentication to facilitate e-banking transactions and other private-sector service exchanges. In 2011, the Government of Estonia reached an agreement with mobile operators to integrate this form of authentication into e-government services as well.

The report went on to relay that users who wished to participate in the mobile identification scheme had to request special PKI-enabled (public key infrastructure) SIM cards from mobile operators and their identity would be verified and a private key stored on the SIM card.

Babakhan follows this line of conversation and says that with GDPR in place, “it is nice to tell customers that they are in charge of their data, but what the consumer actually wants is to know that they can trust in who has access to their data and that it is being used in a proper way.”

He adds: “If you want a successful electronic ID, there needs to be a good technical solution, good security, the ability to process transactions and a platform that offers a wide reach. Banks are in the best position to provide eIDs because we spend a lot of time and money getting to know our clients.”
As identity and money starts to operate and intersect on the same level and stronger, more specific regulations are created as data breaches and hacks seem to increase in number, consumers continue to prioritise trust and are more cautious about handing over their personal information.

The binary opposition of CX and free data

Chris Fletcher, Global Head of Digital and Channel Partners at Western Union Business Solutions, states that while customer trust is imperative within the digital journey, "the holy grail of customer experience is a seamless and frictionless journey but when thinking about trust, it can actually be detrimental.

"Banks need to demonstrate to customers that there is robustness in identity authentication (such as two factor authentication) and that their data is protected through encryption and tokenisation." He added that in the last ten years, the reputation of established banks has eroded and the first barrier that they must overcome, as providers of federated digital identity providers, is to convince their customers that they have learnt from past mistakes.

The adoption conundrum

Speaking of federated digital identity providers, Fletcher pointed out that GOV.UK Verify is still in early stages of adoption and those who are using the service, have had limited success so far. "The number of users is unlikely to reach the 25 million target by 2020. Furthermore, such schemes have had a low success rate in validating users."

The OWI also had more to contribute on this subject. Sarah Clark, principal at the OWI, outlines that, "there is a huge opportunity for banks to become digital identity providers and to play a key role in leveraging their brands and significant mobile banking app adoption levels to increase trust throughout the broad digital economy.

"There are many reasons why banks are well positioned to do this – they already make hefty and growing investments in KYC processes driven by increasing regulation and their own efforts to combat fraud and protect their customers. As a result, they hold some of the best vetted identities from the onboarding process to gain access to a new bank account. These accounts are then continuously monitored and supplemented with valuable banking transaction history that can provide identity assurance or risk signals.

"Mobile app usage rates are high and continuing to grow. This is a strong foundation to attract customers to use a bank-led digital identity system, where a customer can consent to sharing from an app they already have on their mobile device.

"From the bank perspective becoming an identity provider is a highly strategic move, which continues to ensure they will have a strong position at the centre of their customers’ financial and digital lives and can continue to increase the engagement of their own customers, and finally, we know via several surveys of customer sentiment, that there is a relatively high degree of trust in banks."

Breaching consent

OWI’s Kaelyn Lowmaster, head of research, adds: "To borrow a term from Facebook, 2018 was a year full of ‘breaches of trust’. From Cambridge Analytica to mobile location data breaches, consumers this year got a jarring view of how their data is used and shared – often without their understanding or explicit consent.

"On the bright side, that means the fundamental economic bargain of the internet age – data for ‘free’ services – is under new scrutiny. Greater accountability may come from evolving data protection regulations, but pure market pressure – demand for better data stewardship – is already driving companies to take privacy and data protection more seriously."

On a KYC level, regulations such as PSD2 are paving the way for banks to enter the digital identity arena, as financial institutions are required to give access to account data to third parties.
On a KYC level, regulations such as PSD2 are paving the way for banks to enter the digital identity arena, as financial institutions are required to give access to account data to third parties. In order to excel, as well as to comply with regulation, banks may be obliged to work with other complementary private programmes.

Teresa Walsh, Global Head of Intelligence at the Financial Services Information Sharing and Analysis Centre (FS-ISAC), highlights that banks are looking at how these different entities work together.

“The Know Your Customer regulation is extremely important to financial services organisations, and with PSD2 changing the landscape of how firms work with customers, identity is even more critical. This is one of the reasons threat-sharing on fraud is so important. Fraudsters will hit several firms simultaneously, so if we’re not working together to identify the bad guys, they may get away with their crimes. Identity fraud remains a method used by criminals to create false accounts and withdraw money illegally, which can have a long-term impact for legitimate customers.”

Validation as a binary

Following on from this point, Western Union’s Fletcher adds that verification should be thought of as, “different points on a spectrum” and that the “industry often thinks about digital identity validation as a binary outcome – 100% verified or not verified; the person is, or isn’t, who they are claiming to be. However, best practice is moving away from that to determine an outcome based on levels of reasonableness.”

On a KYC level, regulations such as PSD2 are paving the way for banks to enter the digital identity arena, as financial institutions are required to give access to account data to third parties. In addition to this, “the level of digital identity can change over time depending on the tenure of the customer relationships and behaviour. For example, as customers spend more time in an FI’s digital environment, certainty around identity will increase and more functionality can be unlocked.”

OWI’s Sarah Clark also says that, the majority of banks go above and beyond KYC compliance standards in order to protect their organisations against rising digital fraud as well as to protect their customers from becoming victims of identity fraud. We’ve seen banks create innovation centres that are focused on solving KYC and identity needs, with increasing focus on incorporating new technology quickly and effectively – it is generally a strategic imperative receiving ample investment.”

The World Bank and GSMA report provides Nigeria as an example of a country which has produced a national ID in partnership with Mastercard, Visa and a local payment network called Verve. With the aim of streamlining the multiple identity schemes in the African nation, the Nigerian Identity Management Commission (NIMC) began to offer financial services as one application on a smartcard.

The report revealed that due to separate agreements made with local banks, cards can be linked to pre-paid bank accounts and used to make transactions. Following this, databases and services may be linked to a single platform electronic identification, which includes driver’s licenses, voter registration, health insurance, taxes, SIM card registration and pensions.

Source: The Boston Consulting Group (2016)
The importance of digital identities is increasing, and they are becoming our passports to navigate the digital world; therefore digital identity usurpation has an immediate impact and possible financial cost. Banks are building and storing digital identities for their customers and the GDPR is raising new challenges in this respect. Notably, the precise management of the customers’ digital identities and the way to secure them is even more critical as data belongs to the user and not to the bank anymore. Having said that, I think we can expect a strong uptick in demand for digital identity management solutions in the near future.

Do you predict an uptick in demand for digital identity management solutions?

The state of security around digital identities is heterogeneous across the world. In regions like Europe, local regulations are making it mandatory for banks to properly secure the digital identities they manage. However, some banks, for cost reasons, are keeping this security to the bare minimum. In Europe and therefore, banks - even though regulators encourage them to deploy MFA - are hesitant to increase the security level since they are afraid this may impact the UX negatively. Having said that, today progressive technologies can help organizations to implement intuitive UX without compromising with security. In the emerging markets, government identity profiles are not safe and therefore, banks are facing security issues not only in the digital world, but also in the real world. Overall, banks still need to consider advanced security to ensure strong protection of digital identities and continuously improve the trust of their customers by offering innovative digital services.

Would you say that the digital identification being offered by banks is enough?

Digital identities are opening new opportunities on the market and enriching the potential of the services ecosystem. Digital service providers – and banks in particular - need to make sure they know the person conducting transactions with their services. That is why strong authentication of the user is becoming a mandatory step before allowing certain sensitive transactions. As has been reported in the news, hackers have been able to work around some basic strong authentication solutions and that is why it is now even essential to think beyond the classical strong authentication model and consider risk-based authentication approach, where a threat and fraud detection capabilities will complement the authentication method to evaluate the risk of the transactions and detect possible cyber-attacks that could jeopardise the authentication process.

Is there a growing need for stronger customer authentication?

In general banks know a lot about their customers due to their activity. In addition, because of KYC regulations, they must vet customer identities. Today, they store a massive amount of data that could be used to build digital identities of their customers. In addition to this, PSD2 and Open Banking are putting the bank in the middle of the authentication process. There is a great opportunity for banks to extend this critical role of being the trusted authentication service provider in this new extended financial ecosystem and become the trusted digital identity service provider of the full digital ecosystem. Banks possess an authoritative record of everything consumers do – borrowing, lending and spending money on anything from bills and mortgages to travel, food and coffee. Exploring the full potential of this rich information will allow banks to consolidate their position in the ecosystem as a trusted ID provider while placing their customers in the center of the business. Banks can use this valuable information to unlock services that were previously unavailable to customers or only accessible by a specific group of customers. However, to succeed, banks need to be supported with the right technologies and the right partners that will ensure the management and the safety of these digital identities.

Are banks in the best position to offer digital identity solutions, or should they partner with technology providers or governments?

The state of security around digital identities is heterogeneous across the world. In regions like Europe, local regulations are making it mandatory for banks to properly secure the digital identities they manage. However, some banks, for cost reasons, are keeping this security to the bare minimum. In Europe and therefore, banks - even though regulators encourage them to deploy MFA - are hesitant to increase the security level since they are afraid this may impact the UX negatively. Having said that, today progressive technologies can help organizations to implement intuitive UX without compromising with security. In the emerging markets, government identity profiles are not safe and therefore, banks are facing security issues not only in the digital world, but also in the real world. Overall, banks still need to consider advanced security to ensure strong protection of digital identities and continuously improve the trust of their customers by offering innovative digital services.
This directive from the European Commission is resulting in a paradigm shift: data has been given back to the customer. Therefore, the user can ask anything about its own data (consultation, delete, duplication, migration). In addition to this, companies are also taking stronger responsibility to keep data safe because they cannot leverage it without clear user’s consent. This banking ecosystem disruption can only happen if the consumer’s trust is in place and not damaged by fraud. In this regard the PSD2 is bringing a new level of security and requirements for stronger customer authentication, which will help financial institutions to build trust with their customers and therefore empower the adoption of digital services. Multi-Factor Authentication along with Mobile Application Security and Threat and Fraud Detection are now mandatory pieces to insure consumers’ protection and trust.

The financial ecosystem is changing rapidly, and new players are proposing innovative services that are threatening parts of the traditional banking business. What happened with the mobile network operator (MNO) market a few years ago is happening in banking today and digital service providers, called Over the Top (OTT) services, have been leveraging the MNO platforms and services in order to develop their own service and capture most of the value. Banks must reinvent themselves and find new business models to retain their value and as discussed before, this opportunity of being the trusted digital identity provider for the connected world could be a new successful business model.

As financial fraud incidents grow in digital banking channels, it is imperative that institutions protect their customers. This includes securing their browsers, devices and applications while ensuring each transaction can be trusted, from money transfers to adding a beneficiary or requesting a new loan. These requirements are driving a new approach to multi-factor authentication that is based on machine learning and artificial intelligence, allowing organizations to make smarter real-time risk-mitigation decisions while cutting operational costs and reducing fraud-related losses. Deploying intelligent, data-driven authentication methods can optimize the user experience by defining the appropriate level of authentication assurance to be applied depending on the risk level of the user’s environment and transactions. To the extent this can be achieved with high levels of security and an intuitive user experiences, it will create new growth opportunities for financial institutions.

Are we entering a new frontier of privacy and security especially with the introduction of PSD2?

What other challenges do financial institutions have?
The future of biometrics is in behavioural technology which can learn how a user operates and will in turn, build an identification model with software that analyses the way that they interact with different devices, such as their phone, tablet or computer. It can be as intricate and detailed as how they hold the mouse, make keystrokes, the speed at which they move and the pressure that they apply to their phone.

Because these biometrics are interpolated through algorithms to define a unique pattern for each user, it is crucial to the customer onboarding process that this data is collected in a way that does not interrupt the day-to-day actions of the user.

**Onboarding with algorithms**

Biometrics is here to stay. This is clear because of the rapid uptake and acceptance of technology such as Apple’s Touch ID and Face ID. In a recent blog post for Finextra.com, Steve Cook, biometrics and fintech consultant for Biometrics for eCommerce and a recognised thought leader in this field, said: “until 3D face authentication technology became available in late 2017, 2D face recognition that matches two images was all that could be obtained. 2D face recognition vendors promised security but without any proper third-party testing available, it was left to each organisation to perform their own due diligence.”

He continued to say that a problem presents itself when, “2D liveliness detection deployments on the market today can be easily fooled,” and many of the checks that are completed are not secure enough. “Asking a user to blink, smile or nod their head, can all be replicated using photos, video playbacks, masks and even using AI models. These methods can simply bypass virtually all liveliness check systems, especially when it comes to the digital onboarding process.”

While there are several advantages of 3D face mapping technology when it comes to fighting fraud, many new digital only banks are suffering large-scale fraud attacks every day because bad actors have figured out how to get around systems with fake passports and stolen photos.

Cook said that “3D face-mapping contains 100 times more data points than a 2D photo and are required to accurately recognise the correct user’s face while concurrently verifying their human liveliness. This liveliness check is especially critical in unsupervised authentication scenarios such as confidential account access management and high-value mobile transactions. It must be proven in real-time that the person requesting access is the correct user, not just a representation.

“Some businesses are often unable to distinguish a modified recognition product from a true authentication solution, despite the fundamental differences between the two. Some vendors are all too willing to overlook this, which leaves customers and users with a false sense of security and unknown levels of risk.”

**A use case for blockchain**

While biometrics solutions have played a larger part in establishing personal identity solutions and programs, many believe that blockchain may have a bigger part to play. An innovative development would be to establish initiatives that would allow financial institutions to onboard customers by building KYC utilities with blockchain technology.

This would provide a centralised location where client identification and verification can be performed once per person, rather than several times by different organisations for the same customer.

According to a PwC report on identity and KYC, ‘Digital identity: Changing the way financial institutions connect with customers’; “digital identity solution

---

11 Steve Cook for Finextra, ‘3D face mapping as a true differentiator in biometric liveness detection’ (2018).
While biometrics solutions have played a larger part in establishing personal identity solutions and programs, many believe that blockchain may have a bigger part to play. An innovative development would be to establish initiatives that would allow financial institutions to onboard customers by building KYC utilities with blockchain technology.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.

The Singaporean case study

However, the most notable use of blockchain technology in identity services has been in Singapore. As written by Paul Bryzek on Medium in his article ‘How Blockchain is used by Governments as a form of National Identity,’ the city-state is attempting to upgrade their existing electronic government service, SingPass.

The Monetary Authority of Singapore also partnered with distributed ledger technology company R3 to conduct inter-bank payments and could transfer this knowledge to the identity market, as suggested by Rabobank’s Ali Babakhan and Daan Van Den Eshof.

Kaelyn Lowmaster, Head of Research, OWI highlights that while blockchain can solve some problems with digital identity, it cannot solve all of them. “Blockchain could help make transacting identity data more secure and user-centric, but it definitely doesn’t help with creating digital identities. There’s still a real garbage-in, garbage-out problem with distributed ledger technologies.

“Plus, blockchain is all about disintermediation - making sure there’s no central authority guaranteeing transactions. But we don’t yet have a great solution for authority-free identity creation. You can put your government credentials in a blockchain-based wallet, but you’re still fundamentally using government credentials. In short, disintermediation isn’t always a good thing, and blockchain technology still has a long way to go when it comes to national identity systems.”

Interestingly, adoption has been notable in India after critics slammed the centralised nature of Aadhar and the subcontinent is looking to release a second version that would be secured by an immutable blockchain to prevent future data breaches.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.

Based on blockchain or distributed ledger technology (DLT) is economical, immutable, secure and easily accessible, while also providing a legitimate audit trail.

“The advantage of a DLT-based identity system over traditional ones is its ability to record each identity shared in the global network and to maintain continually reconciled data throughout the network.”

The report went on to say: “The institution can then share customers’ data with other entities for legitimate purposes, only after receiving the customer’s consent. This facility benefits all parties in saving time and money by eliminating the need for KYC at multiple places within or outside the country, thereby optimising costs involved in accurately establishing identities. With a single identity across the globe, it also aids regulators to monitor fraudulent activities, such as money laundering, more effectively.”

Based on blockchain or distributed ledger technology (DLT) is economical, immutable, secure and easily accessible, while also providing a legitimate audit trail. “The advantage of a DLT-based identity system over traditional ones is its ability to record each identity shared in the global network and to maintain continually reconciled data throughout the network.”

The report went on to say: “The institution can then share customers’ data with other entities for legitimate purposes, only after receiving the customer’s consent. This facility benefits all parties in saving time and money by eliminating the need for KYC at multiple places within or outside the country, thereby optimising costs involved in accurately establishing identities. With a single identity across the globe, it also aids regulators to monitor fraudulent activities, such as money laundering, more effectively.”

Interestingly, adoption has been notable in India after critics slammed the centralised nature of Aadhar and the subcontinent is looking to release a second version that would be secured by an immutable blockchain to prevent future data breaches.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.

The Singaporean case study

However, the most notable use of blockchain technology in identity services has been in Singapore. As written by Paul Bryzek on Medium in his article ‘How Blockchain is used by Governments as a form of National Identity,’ the city-state is attempting to upgrade their existing electronic government service, SingPass.

The Monetary Authority of Singapore also partnered with distributed ledger technology company R3 to conduct inter-bank payments and could transfer this knowledge to the identity market, as suggested by Rabobank’s Ali Babakhan and Daan Van Den Eshof.

Kaelyn Lowmaster, Head of Research, OWI highlights that while blockchain can solve some problems with digital identity, it cannot solve all of them. “Blockchain could help make transacting identity data more secure and user-centric, but it definitely doesn’t help with creating digital identities. There’s still a real garbage-in, garbage-out problem with distributed ledger technologies.

“Plus, blockchain is all about disintermediation - making sure there’s no central authority guaranteeing transactions. But we don’t yet have a great solution for authority-free identity creation. You can put your government credentials in a blockchain-based wallet, but you’re still fundamentally using government credentials. In short, disintermediation isn’t always a good thing, and blockchain technology still has a long way to go when it comes to national identity systems.”

Interestingly, adoption has been notable in India after critics slammed the centralised nature of Aadhar and the subcontinent is looking to release a second version that would be secured by an immutable blockchain to prevent future data breaches.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.

The Singaporean case study

However, the most notable use of blockchain technology in identity services has been in Singapore. As written by Paul Bryzek on Medium in his article ‘How Blockchain is used by Governments as a form of National Identity,’ the city-state is attempting to upgrade their existing electronic government service, SingPass.

The Monetary Authority of Singapore also partnered with distributed ledger technology company R3 to conduct inter-bank payments and could transfer this knowledge to the identity market, as suggested by Rabobank’s Ali Babakhan and Daan Van Den Eshof.

Kaelyn Lowmaster, Head of Research, OWI highlights that while blockchain can solve some problems with digital identity, it cannot solve all of them. “Blockchain could help make transacting identity data more secure and user-centric, but it definitely doesn’t help with creating digital identities. There’s still a real garbage-in, garbage-out problem with distributed ledger technologies.

“Plus, blockchain is all about disintermediation - making sure there’s no central authority guaranteeing transactions. But we don’t yet have a great solution for authority-free identity creation. You can put your government credentials in a blockchain-based wallet, but you’re still fundamentally using government credentials. In short, disintermediation isn’t always a good thing, and blockchain technology still has a long way to go when it comes to national identity systems.”

Interestingly, adoption has been notable in India after critics slammed the centralised nature of Aadhar and the subcontinent is looking to release a second version that would be secured by an immutable blockchain to prevent future data breaches.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.

The Singaporean case study

However, the most notable use of blockchain technology in identity services has been in Singapore. As written by Paul Bryzek on Medium in his article ‘How Blockchain is used by Governments as a form of National Identity,’ the city-state is attempting to upgrade their existing electronic government service, SingPass.

The Monetary Authority of Singapore also partnered with distributed ledger technology company R3 to conduct inter-bank payments and could transfer this knowledge to the identity market, as suggested by Rabobank’s Ali Babakhan and Daan Van Den Eshof.

Kaelyn Lowmaster, Head of Research, OWI highlights that while blockchain can solve some problems with digital identity, it cannot solve all of them. “Blockchain could help make transacting identity data more secure and user-centric, but it definitely doesn’t help with creating digital identities. There’s still a real garbage-in, garbage-out problem with distributed ledger technologies.

“Plus, blockchain is all about disintermediation - making sure there’s no central authority guaranteeing transactions. But we don’t yet have a great solution for authority-free identity creation. You can put your government credentials in a blockchain-based wallet, but you’re still fundamentally using government credentials. In short, disintermediation isn’t always a good thing, and blockchain technology still has a long way to go when it comes to national identity systems.”

Interestingly, adoption has been notable in India after critics slammed the centralised nature of Aadhar and the subcontinent is looking to release a second version that would be secured by an immutable blockchain to prevent future data breaches.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.

The Singaporean case study

However, the most notable use of blockchain technology in identity services has been in Singapore. As written by Paul Bryzek on Medium in his article ‘How Blockchain is used by Governments as a form of National Identity,’ the city-state is attempting to upgrade their existing electronic government service, SingPass.

The Monetary Authority of Singapore also partnered with distributed ledger technology company R3 to conduct inter-bank payments and could transfer this knowledge to the identity market, as suggested by Rabobank’s Ali Babakhan and Daan Van Den Eshof.

Kaelyn Lowmaster, Head of Research, OWI highlights that while blockchain can solve some problems with digital identity, it cannot solve all of them. “Blockchain could help make transacting identity data more secure and user-centric, but it definitely doesn’t help with creating digital identities. There’s still a real garbage-in, garbage-out problem with distributed ledger technologies.

“Plus, blockchain is all about disintermediation - making sure there’s no central authority guaranteeing transactions. But we don’t yet have a great solution for authority-free identity creation. You can put your government credentials in a blockchain-based wallet, but you’re still fundamentally using government credentials. In short, disintermediation isn’t always a good thing, and blockchain technology still has a long way to go when it comes to national identity systems.”

Interestingly, adoption has been notable in India after critics slammed the centralised nature of Aadhar and the subcontinent is looking to release a second version that would be secured by an immutable blockchain to prevent future data breaches.

Blockchain presents a good way to track ownership and identity in a digital world without imperial powers or governmental power and is becoming the favoured technology for proving ownership. With such a focus on privacy, blockchain could be a way of solving some of the current issues.
Expert view:

Frederik Mennes
Senior Manager, Market and Security Strategy, Security Competence Centre

In a Q&A interview with OneSpan, Frederik Mennes, senior manager market and security strategy, security competence centre, highlights what is happening regarding identity in the European Union, where banks play a part and how much regulation has made an impact.

Strong Customer Authentication (SCA) is an act of authentication that uses at least two out of the three factor categories: what I know, what I have and what I am. These factors need to be mutually independent. A user must be informed of the transaction details, and the authentication process must result in a unique code linked to these transaction details.

According to Article 97 of PSD2, PSPs should apply SCA when customers access their online payment accounts, no matter if they want to perform a monetary transaction or other types of operations, like adding a trusted beneficiary. It will also be obligatory for any actions performed through a remote channel that may carry a risk of fraud, like accessing a bank account via a mobile device. In some cases, PSPs may be exempted from applying SCA.

In the EU we are seeing several regulations developing in digital identity verification. PSD2, Strong Customer Authentication and its technical standards is one of the key drivers of change in Europe. The eIDAS regulation is also harmonising the usage of electronic identity cards throughout EU. The 5th European Anti-Money Laundering regulation that is also coming up contains requirements for banks to perform identity verification during account opening.

Digital identity will become more common place in the account opening process and we are not too far away from having to do every type of transaction from our computer or mobile device. We will also see a large adoption of government issued identity cards and passports for use in financial services. Because of this adoption, we will have a centralised authentication means to log on to different accounts from financial institutions. We are already seeing this adoption in other countries such as Netherlands, Belgium and Singapore. Finally, we’ll see an uptick in the adoption of continuous adaptive authentication because users want to access online banking applications without any friction or hurdles to authenticate the user.

Do you predict an uptick in demand for digital identity management solutions?

Banks will play an important role in digital identity solutions, not only for their own applications but for the applications of other organisations. For example, e-commerce providers can delegate the authentication of its users to financial institutions. Additionally, the government can also play an important role as they are deploying more digital identity cards.

Should banks partner with technology providers or governments to provide identity services?

In the EU we are seeing several regulations developing in digital identity verification. PSD2, Strong Customer Authentication and its technical standards is one of the key drivers of change in Europe. The eIDAS regulation is also harmonising the usage of electronic identity cards throughout EU. The 5th European Anti-Money Laundering regulation that is also coming up contains requirements for banks to perform identity verification during account opening.

Is regulation enough for banks to do due diligence on their customers?

Strong Customer Authentication (SCA) is an act of authentication that uses at least two out of the three factor categories: what I know, what I have and what I am. These factors need to be mutually independent. A user must be informed of the transaction details, and the authentication process must result in a unique code linked to these transaction details.

According to Article 97 of PSD2, PSPs should apply SCA when customers access their online payment accounts, no matter if they want to perform a monetary transaction or other types of operations, like adding a trusted beneficiary. It will also be obligatory for any actions performed through a remote channel that may carry a risk of fraud, like accessing a bank account via a mobile device. In some cases, PSPs may be exempted from applying SCA.

How do you benefit from being offered Strong Customer Authentication by banks?
What do you see for the future of privacy?

In the future, I expect authentication methodologies to become more privacy aware. Today when we share data with financial institutions and other companies we share a lot of personal data about ourselves, but maybe that’s not necessary as we investigate the future. Privacy enhancing technology will become more common and limit the amount of personal data that users share about themselves. On the other hand, financial institutions need to strike a balance between security and user convenience. Fraudsters will always be active wherever there is data and money. Recently, we’ve seen fraudsters target mobile banking channels with a new threat known as overlay attacks. As banks roll out more mobile banking apps, we expect fraudsters will target that channel more and more.

How can you help banks improve their KYC and onboarding processes?

Banks can leverage digital identity verification solutions to verify applicants in real-time during the onboarding process. There are many ways to carry out KYC checks during the account opening process. This often depends on the type of transaction and associated risk, geography and industry regulations. At its core, KYC ensures that the applicant is who they say they are and that they are not attempting to enter into an agreement illegally or fraudulently.

Look for solutions that will enable your bank to:

- Check the authenticity of government-issued ID documents (e.g., driver’s license, passport, etc.), especially for remote, unmediated applications
- Verify the identity of the applicant using biometric (“selfie”) verification that ties the applicant to the photo on the ID document
- Automate customer due diligence checks with third-party credit bureau providers to meet Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements
- Pre-populate application fields with the applicant’s information and capture consent with e-signature
- Capture comprehensive audit trails – from ID verification to signature – in a single evidence package
- Offer an intuitive user experience – across all your digital channels
Digital verification and authentication in banking is undergoing fundamental change. Due to increasing expectations from both customers and regulators, financial institutions are struggling to keep up with the technological innovation being offered by Big Tech. Another obstacle also presents itself when digital identity services create a new entry point for hackers.

However, it has been continually reiterated that being able to prove your identity should be made a priority across the world, but cultural aspects may hinder or prevent national initiatives from being established. While there has been a remarkable uptick of digital identity service users in developing countries, interest from UK and US citizens has waned.

The concept of trust was widely debated in 2018 and filtered through to the identity conversation, where industry experts discussed whether it should be the government that should provide ID services, financial institutions or if it should be a collaborative approach.

Research while compiling The Future of Personal Identity report 2019 found that while people do not often change their bank, politicians come and go and as a result, a trusted entity needs to produce credentials that allow people to become trusted citizens, and banks could be these trusted custodians.


This report is published by Finextra Research.

Finextra Research is the world’s leading specialist financial technology (fintech) news and information source. Finextra offers over 115,000 items of specialist fintech news, features and TV content items to 420,000 unique monthly visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra’s unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

Finextra reports coming in 2019:

The Future of Artificial Intelligence
The State of Fintech
The Future of Payments
The Future of Trade Finance
The Future of Dev Ops
The Future of Core Banking
The Future of Treasury
The Future of Cyber Security

Contact Salesadmin@finextra.com to get involved.