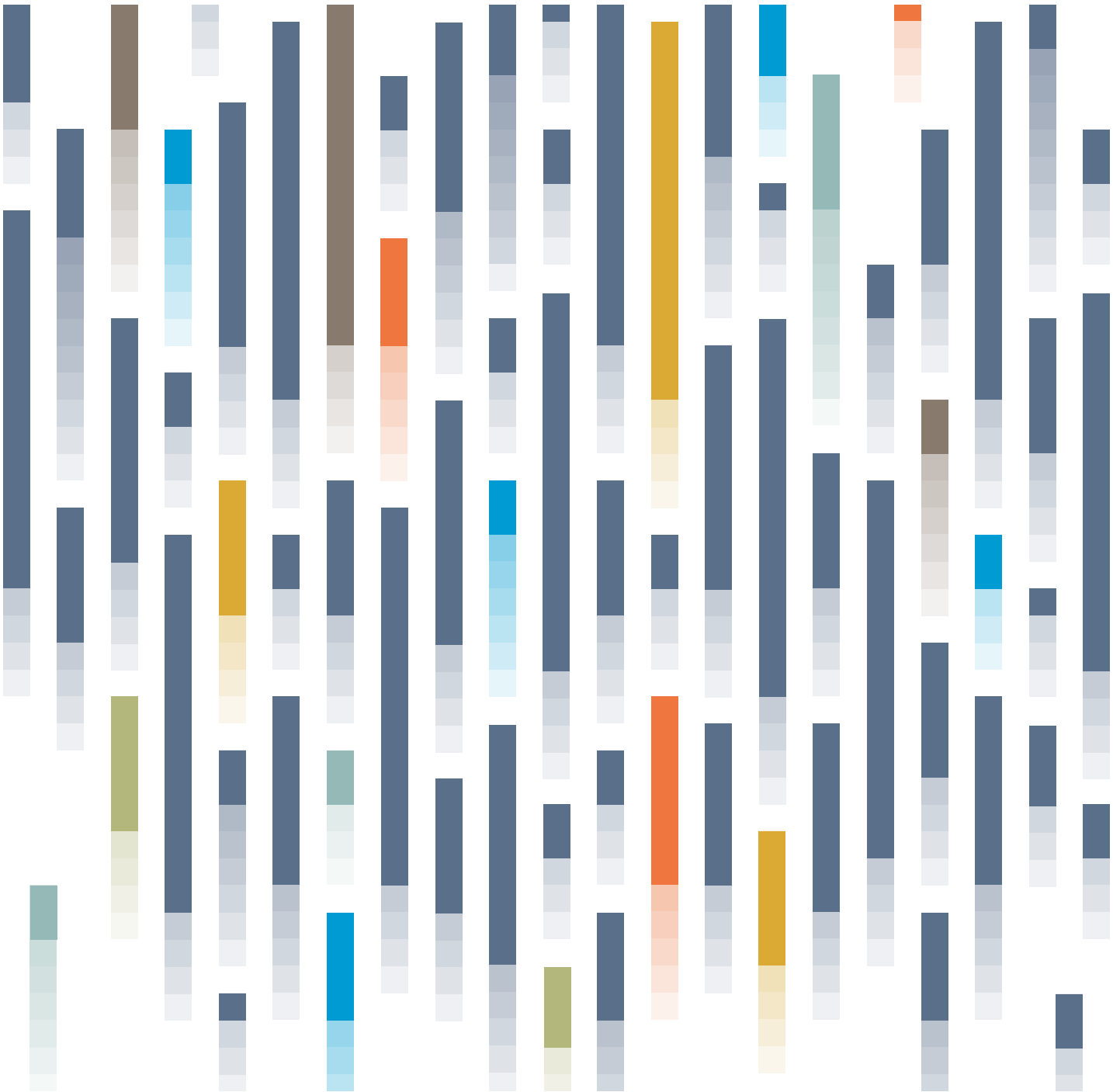
UBS

Digital Identity

A UBS Group Innovation White Paper



Introduction

The Internet ushered in a revolution in communications. With it we could instantly share information, and most of anything else that could be digitized, with almost anyone in the world. The result was an explosion in productivity and interconnectedness.

But while the Internet supports sharing information, it is less capable of verifying the source and validity of the data. This has led to all kinds of problems, from fraud to phishing to phony news. The lack of an authentication layer, while convenient, also means the Internet is not a particularly secure channel for transactions.

This might seem surprising in an age when e-commerce is booming. The truth is, when we use our browsers to buy something online, we are only sending information – our name, credit card number, etc. That information still needs to be verified and processed in the old ways; e-transactions are not truly online.

If we want to have a fully digital economy, we will need to have truly digital identities. As a bank we know this all too well. Identity has been a core part of our business since the beginning. Today we are, we think, rather good at verifying, safeguarding and using identities in the analog world. The great challenge now is to do this digitally and seamlessly.

Our world is digitalizing at a fast pace, and we can begin to see the outlines of what a fully digital economy might look like. But we see many hurdles too. Part of the problem is that we still rely to a great extent on the analog world – as when asked to produce a physical passport or birth certificate to open a bank account. Our identities are also complex. From our name, address and date of birth to our preferences in clothing and circle of friends, all the information about us can be used in one way or another to identify us. There are also serious problems in the way identity is currently handled in the digital realm, from lack of security of our data to lack of control over it.

Such problems are understandable in a period of transition like ours. And as identity will play such a key role in our digital future, we can expect a great deal of resources to go into solving them. We see already that digital identity is a hot topic among governments and regulators, banks and tech companies, NGOs and academics. And there are projects underway all over the world to build better digital identity solutions. We expect these efforts to intensify.

In our view, these developments will slowly but surely lead to a broad-based, regional and perhaps global digital identity platform. We can picture this as a base layer for securely collecting, verifying and sharing identity that is as unobtrusive, yet as powerful, as the communications layer that underpins the Internet itself.

What such a platform will ultimately look like is very much in the open. In this paper we take you on a journey through this digital evolution – and so explore its possible futures and what they might mean for us as banks, for our clients, and for the world at large.

Foreword

In January of 2016 we published a paper for the meeting of the World Economic Forum about the coming fourth industrial revolution.

In it we suggested that if the first three industrial revolutions took us from steam engines to mass production to our modern IT and communications, this new age would bring us a world of extreme automation and connectivity. As with the first three such revolutions, this would be the catalyst of profound change.

Since then we have been examining the coming fourth industrial revolution in more detail from a number of different angles.

In mid-2016, we published a major white paper on the blockchain, a new technology, very much in the fourth industrial revolution mold, that we believe may cause massive disruption and transformation to, and beyond, the global financial system.

In the fall of 2016 we launched our Future of Finance Forum series. At these events we bring together leaders and experts from academia, blue-chips, fintechs and regulators to look at aspects of how the fourth industrial revolution may play out in our economy and society and financial services in particular.

We chose digital identity as a key topic for our Future of Finance series because identity is one of the most important elements of any economy, and because it will not be possible to build a fully digital economy without collaboration from market participants to establish identity online.

This paper is intended for a general audience. It is part of our ongoing efforts to provide information and insight on important topics to those for whom we provide services, as well as to society at large.

We hope you will find it thought provoking reading.

Axel P. Lehmann
UBS Group Chief Operating Officer

Authors

Anthony Clark-Jones
Innovation Partnerships Manager
UBS Group Innovation

Giulia Fitzpatrick
Managing Director
UBS Wealth Management

Martin Hartenstein
Head of Strategy and Business Transformation
UBS Wealth Management

Alain Hiltgen
Head of Business Security Advice
UBS Group Technology

Veronica Lange
Head of Innovation
UBS Group Innovation

Andreas Przewloka
Group Managing Director
UBS Wealth Management

Marzia Thüring-Menegon
Managing Director
UBS Wealth Management

Paul Yardley
Innovation Experiment Lead
UBS Group Technology

Table of contents

Identity today

In today's digitizing world, our identities are increasingly defined by a complex web of personal data – provided, collected and shared by innumerable entities. While often useful, current identity systems struggle at times to give us the security, control and ease of use we should expect.

The key to the (digital) highway

Establishing identity is one of the key prerequisites for a functioning economy: You can't hold someone's wealth in an account without knowing who they are; you can't have transactions without being sure of the counterparties.

We've come a long way since Renaissance bankers relied on personal relationships or wax-sealed letters of introduction to verify identity. Today our financial system connects an unfathomable number of people, organizations, assets, and financial instruments in a dynamic, intricate web. To carry out transactions and make our economy flow, all these entities need to be repeatedly, uniquely and correctly identified as they make their way through the system.

Doing so is a challenge today. As we work towards developing a fully digital economy, the challenges will only increase.

For one, the number of entities in the system is set to explode. As we further globalize, more regions of the world – meaning more people and organizations – will come online. As the Internet of Things grows, there will also be an explosion of objects, from refrigerators to shipping containers, coming online as well. If all of these entities are to transact seamlessly with each other, we must have standard ways of establishing and verifying who and what they are.

But it's not just a question of numbers. As our world digitizes, many processes will become more automated. Developments like the blockchain, smart contracts and artificial intelligence will allow machines and other objects to become economic actors in their own right.

A smart contract can be thought of as shared code that executes autonomously, often on a blockchain. It can be used to store value (money) and be programmed to make decisions about what to do with it. To be effective it will need access to an identity system that is not only foolproof, but which works without human intervention.

For this and other reasons, digital identity can be seen as the nucleus of a digital economy – the glue which binds its parts, and the key which unlocks its potential. It is imperative therefore that we make it work.

The puzzle in the mirror

In today's world, our identities consist of a large collection of pieces of information. Some of these can be considered part of our "core" identity, for example our name, our date of birth, or our gender – the basic information society requires of us in order to identify ourselves in public.

On top of this we have different layers of identity "attributes." Some are "biometric," like our face, our fingerprints, our voice patterns, or even our DNA. Some are official, like our citizenship status, driver's license, credit card or other account numbers. Some are social, like who we are married to, our children's names, our circle of friends, our tastes in food, clothing, hobbies, and so on. Put all of this data together and we get a good picture of who we are.

Except for our intrinsic biological traits, most of these attributes are assigned to us or collected in one way or the other. It begins when we are born and continues as we travel through life until we pass away (and, in some places, receive a certificate confirming our death).

Today there are countless entities that assign attributes. Some are obvious, like governments, banks, credit card companies, or even doctors. But by collecting information about us, social media sites, telecommunications companies, search engines, not to mention all the websites we visit, in essence assign us attributes as well – whether we know it or not.

The many faces of me

In general we do not want to share all our identity attributes with everyone. And so we prefer if possible to bundle our attributes into various groups or "personas," each appropriate to a different context.

For example, we may want to share a set of attributes only with our doctors (health records, dietary habits), another set with online vendors (credit card number, age) and so on. This makes it desirable to be able, if possible, to control and selectively use our identity attributes.

While by themselves these attributes may have no intrinsic value, they do have a value in terms of what they enable us to do. Without a valid citizenship attribute (passport, voter registration), we cannot travel abroad or participate in our country's political future, and without a valid credit card attribute we cannot, for example, rent a car.

Our attributes also have a value in terms of what they enable others to do. Today companies collect a great deal of information about us in order to be able to serve us better, or to generate income – most commonly through marketing. We could imagine a future in which the roles will be reversed, and we control our identities and sell our data to companies. In such a world, digital identity would have a very tangible value.

Identity crisis

While we have come a long way in the last twenty years in the development of online communications, there are still a number of serious problems with the way digital identity is handled. Among them:

Identity is not secure enough. Major hacks resulting in the release of private information are increasingly common, and identity theft is widespread. Today's online identities leave people concerned with regards to how secure they are for important private matters.

Identity is redundant. Identity systems do not communicate well with each other, as we experience every time we have to register for yet another website, or produce the same documents – yet again – when we open a new bank account.

Identity is not standardized. Redundancies are a product of the fact that we have no standard means to assign, list or share identities. Each identity provider, whether a government, bank or phone company, stores identity information in its own way.

Identity is fragmented. Information about us is gathered and stored in many different places, from government and bank databases to those of marketers and criminals.

Identity is not under our control. Related to the above, it is difficult if not impossible for us to have an overview of who holds what information about us. Once in the digital world, information about us can be very easily held, copied and used without permission.

Identity governance is neither complete nor harmonized. Many legal issues touching identity remain to be addressed, for example who is liable for data breaches? And while regulators in some jurisdictions have been addressing identity issues, the legal or regulatory framework is by no means complete nor harmonized.

Identity is not universal. There are millions of people in the world who have no official identities and as a result are often excluded from the benefits and protections of society. In a digital economy, lack of such credentials will make them even more excluded.

The good news is that change is in the air. The growing momentum of the fourth industrial revolution and the increasing move to a digital economy is driving awareness of identity issues among the public, academia, governments and the private sector.

We are also seeing a number of significant technological advances – from the blockchain to biometrics – which could play significant roles in overcoming the above issues and making future digital identity platforms viable.

For these reasons, we think we may have reached an inflection point on the path to a solution.

"A successful e-Identity system will allow users to easily manage their different identities across different organizations and will protect the users' on-line privacy."

Jan Camenisch, IBM
Future of Finance Forum participant

Across the seas

In these days of globalized markets we are so used to carrying out transactions across borders that we can lose sight of the complexity.

Typically when a company or individual sends money abroad, to purchase goods and services or send money to friends or relatives, the transaction passes via several payment rails from the originating bank through a number of correspondent banks to the receiver's bank. While there are some emerging fintech solutions to help streamline the process, using banks for international transactions can take several days before settlement.

One reason – though by no means the only – for the delay is the various requirements associated with accurately identifying counterparties. Because there are no standard means in place to share identity information, and because the laws and regulations can be different across jurisdictions, each institution along the chain often has to "start from scratch" when identifying who is who, and this can include complex Know Your Customer and anti-money laundering checks. If information is missing, ambiguous or erroneous, further (often manual) checks need to be made. This adds to the delays and the costs, not only because the current system is liable to fraud and other human error.

If there was a way to have a trusted, secure and universally accepted digital identity for both the sending and receiving party then the process could be streamlined, error rates reduced, and regulatory compliance made easier. That could result in significant cost savings, time savings, increased trust and reduced fraud, as well as a better customer experience. It may also generate additional revenue streams through offering a more compelling client experience. Solving the digital identity challenge could make this a reality.

Examples of digital identity initiatives

Canada
Digital ID and Authentication Council of Canada (DIACC)
Created as a result of the government's Task Force for the Payments System Review, the DIACC is a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation the global digital economy. DIACC members include representatives from both the federal and provincial levels of government as well as private sector leaders. A prominent digital identity provider in Canada is SecureKey.

Sweden
BankID
BankID is a citizen identification solution that allows companies, banks and government agencies to authenticate and conclude agreements with individuals over the internet.

Finland
TUPAS
TUPAS is an identity system in Finland where all leading Finnish banks are digital identity providers. Individuals can log into a wide range of services via their banking credentials.

UK
GOV.UK Verify
GOV.UK Verify provides a single trusted login across UK Government digital services. People choose from a number of government-approved 'identity providers' – this provider checks the individual is who they say they are when they sign up, authenticates their identity, and provides an easy way for them to log back in every time they sign onto a government service. GOV.UK Verify offers a consistent way to prove identity when accessing government services online.

India
Aadhaar and Digi Locker
Aadhaar is a unique 12 digit number given to every Indian citizen using biometric inputs. It can act as an individual's identity verification and also help them access Government services seamlessly. India is also working towards paperless governance through Digi Locker. A highly secure cloud based platform, Digi Locker provides the opportunity to organisations and individuals to issue, verify, store and access all their legal documents.

Denmark
NemID
NemID is a national electronic ID and digital signature infrastructure that has been developed in close cooperation with the banking sector and is operated by a private provider for the government and Danish banks. The system, which is provided free of charge to Danish citizens, offers a common identification method for citizens to access both public and private services.

Estonia
e-Residency
e-Residency is a transnational digital identity available to anyone in the world interested in administering a location-independent business online. Additionally, e-Residency enables secure and convenient digital services that facilitate credibility and trust online.

The road ahead

Technological change tends to follow a pattern: individual efforts and small projects push the technology forward, leading to ever-larger platforms and eventually consolidation and broad-based standards. We think this will likely be the case for digital identity.

Our goal for identity in the digital economy is clear: We want the means to unambiguously identify all the people and things that interact within it, in a way that is safe and secure and allows these actors to share only the attributes necessary for a transaction, while giving the counterparties strong assurance that those attributes are authentic.

How do we get there? If the history of technology is any guide, the evolution of such a broad-based digital identity framework is likely to go through several phases.

You go your way; I'll go mine

In a first phase we envisage individual stakeholders or groups working on solutions to specific digital identity problems or use cases – as indeed is happening today.

Governments for instance have a strong interest in identity to help them service, protect and understand the needs of their citizens. We already see innovative e-government solutions like the e-ID in the Nordic countries, the GOV.UK Verify program in the UK, or the versatile e-Identity card in Estonia. We can and should expect more.

Regulators are taking an interest in digital identity as a way to protect consumers and stabilize markets, and will increasingly look to write rules that do so. The recent General Data Protection Regulation (GDPR) in the EU, a broad-based regulatory effort to help protect the personal data for EU citizens and provide a unified regulatory environment for identity within the region, is a prime example.

Non-governmental and international organizations, like the UN's ID2020 project or the Global Identity Foundation, are taking an interest in digital identity to address the needs of developing nations and the world's poor, many of whom are excluded from the digital economy due to lack of credentials.

Private sector companies have a great need for comprehensive and scalable digital identity systems, whether to manage and understand their myriad relationships with customers, suppliers and partners, or provide customers with easy and secure access to ever more online services.

Companies like Microsoft, SAP, Oracle or Salesforce cater to this need with sophisticated CRM and related identity services. Google, LinkedIn or Twitter and others, whose business models are to a large extent based on the collection and management of identity data, are finding ways to extend their services and expertise to third parties – as when you use your Facebook login to access a non-Facebook application.

Industries as a whole are also unlocking the digital identity challenge, often through consortia. The TUPAS system in Finland, for example, was created by the Federation of Finnish Financial Services to provide a de facto identity standard for the customers of all Finnish banks.

There's an App for that

There is no reason to think that such efforts won't intensify as the pace of digitalization increases around the world. This in turn will drive advances in core technologies and methods of relevance to future identity platforms.

We will, for instance, very likely see biometric techniques continue to mature as a means of authentication. Using finger prints to unlock your smart device is already commonplace. Technologies are now being developed to do similar things with other biological markers, like our retinas, heartbeats, vein patterns, voices or even DNA.

Behavioral and geographic metrics can also function as a means of authentication. Where we are when we access information is one technique already in use, as anyone knows who as logged into Google or iCloud from a new location. Technology that monitors the way we use our devices – how we hold them, how we use the keyboard – is also becoming available, and can be used to check if it is really us at the controls.

Our social lives can function as markers of identity as well. Social graphs – the maps of our network of social and professional connections – can for instance allow us to easily differentiate "John Smith" of London, England from "John Smith" of London, Ontario, without having to ask either to supply any information.

We also predict that developments in cryptography and related fields will continue to contribute to our ability to securely authenticate, store and share information, including personal data. In this context special mention must be made of blockchain technology (which we have explored in a previous white paper), as it offers a number of intriguing capabilities which could be used to develop decentralized, open source identity platforms.

Finally, artificial intelligence (AI) in its various forms will likely be employed in many areas of identity. As a means of analyzing large amounts of data and finding patterns, AI can play a role in fraud detection through spotting anomalous behaviors. It can also help companies pull together large sets of identity attributes to evaluate risk or carry out customer segmentation.

More, please

As these and other developments lead to increased use of digital identities, we can expect awareness of how identity can function in the digital economy to grow among those who use it.

Much of this is likely to leave a positive impression.

As broader-based digital identity systems come into place, people will begin to see their advantages in terms of convenience and – if done right – security. As we learn more about how to safely share credentials, companies will be able to offer increasingly appealing and seamless customer experiences. In our view, this will drive demand for more of the same and, importantly, raise minimum expectations of what identity solutions should offer.

We can expect similar enthusiasm from governments and the private sector, particularly as the efficiency benefits of digital identity platforms become clearer. By one estimate, for example, the aggregate cost of managing digital identity in the UK in its current fragmented state costs upwards of three billion British pounds a year. Standardization could easily reduce this to 150 million[1], and would certainly mitigate the costs of identity fraud borne by banks and other Financial Services providers. That's a strong incentive.

"A robust digital identity infrastructure is crucial for the future of Internet based transactions, one that integrates the scalable sharing of personal data in a privacy-preserving manner as the basis for highly secure digital identities. Distributed trust authorities on the Internet, supported by distributed safe computations on peer-to-peer networks and blockchains, will increasingly become foundational features of this future infrastructure. We are delighted to see UBS spearheading this effort in the global financial community towards a future Internet with a robust digital identity infrastructure."

Thomas Hardjono, MIT
Future of Finance Forum participant

1 "Economics of Identity: The size and potential of the UK market for identity assurance" by Alan Mitchell and Jamie Smith © The Open Identity Exchange. Published in June 2014.

Not so fast

On the other hand, people will likely also become increasingly aware of the problems that can arise when our identities reside online.

We have already said that security is a major concern. In a fully digital economy identity theft will only become far more dangerous than it is now, making such concerns acute. Continued high-profile hacks – including state-sponsored attacks of the type reported lately – and a large increase in the numbers of people suffering as result, will likely intensify calls for more secure systems and slow down adoption of the less secure.

Today we are used to companies wanting to collect as much information about us as possible. Data breaches in an increasingly digital economy may, paradoxically, reverse this trend. Companies that collect data on us could be mandated by law to keep it secure, and be held liable if they cannot. That could turn personal data into both an asset and a liability that, far from collecting, companies may look to offload.

As companies collect more information about us, there is a greater chance that spurious data enters their systems without our knowledge, erroneously influencing their decisions. We can expect this to lead to more and more problems for consumers, and so drive calls for more control by individuals over their data. We think it likely that awareness of digital identity issues will increase calls for privacy and anonymity online, along with increased ease in sharing identity attributes when desired.

We should also remember that people won't be the only beneficiaries of the digital economy. As the Internet of Things matures, our machines – from refrigerators to shipping containers – will become increasingly autonomous actors. That will make it more important that they know who we are. It might be an amusing anecdote if we can't identify ourselves to our smart home when we return from a night out; less so if our self-driving car thinks we are someone else.

Creative muddle

We envisage that the combination of use-case specific projects, improving technology and pressure from users will move identity platforms forward. As a result, we should expect growing sophistication, better security and increasing interoperability driven by standards and competition.

This is already happening. The Finnish TUPAS system, devised by banks, can also be used to access government services. SecureKey in Canada, another identity platform used by banks, recently said it was expanding to become a national identity platform for accessing a wide range of public and private services[2].

But the fact remains that this evolution looks to be piecemeal. It will likely result in a mix of identity platforms of different shapes and sizes, used in different regions and industries, based on different technologies and standards, and offering differing levels of security and convenience. This starts our journey, but it's still not the final destination.

2 www.securekey.com

We know you!

Many of us have likely had this experience: we go to open a bank account and are requested to bring with us one or a number of “proofs” of identity. These are often physical documents, like a passport, utility bill or tax record. Once the bank verifies the information, we are “on boarded” onto its systems and can access its products and services. But what happens if we want to open an account at a different bank? Almost always, the answer is we have to go through the process again.

This may not seem like too much of a hassle, but played out over the millions of accounts and relationships opened between banks and their customers, such repetition adds significant cost and complexity into the system.

A digital identity solution could streamline this procedure by allowing customers to hold and control access to digitalized versions of the identity proofs themselves. Here is how it could work:

Let's assume a user has a mobile application, call it a wallet. The wallet locally stores a copy of the passport (scanned image), a copy of a utility bill and a copy of a tax bill. The user opens the first bank account and provides the original documents to the bank. The bank verifies the documents, makes a digital copy of the document and then digitally signs it. This acknowledges that the bank has seen the original document and that it reflects the information that it has on file for the wallet holder. This “signed” copy is then passed back to the customer's wallet.

When the customer moves to the second bank they can decide to present some or all of the documents already “signed” by the first bank to the second bank via the wallet. The customer can even choose to present only particular sections of the information, say their nationality from the passport but not the date of birth. Since the document contains a digital proof that the first bank has seen the original identity documents, the second bank can decide whether to rely on that for its own verification purposes. Since this is a 100% digital transaction, it is also very convenient.

We can take this approach one step further. A proof of address, for example, could be issued and signed directly by a utility company. The banks involved would therefore not necessarily have to trust each other, but instead the authority that issued the document, with shared attestations and notarization on the blockchain a potential development here. This not only makes things more efficient, it also makes the digitally-signed documents in the customer’s wallet more reliable as only those entities which are the undisputed authorities in their areas would be qualified to digitally sign the relevant documents.

Future states

As digital identity matures, new needs will arise in the identity ecosystem – along with new products and services to cater to them. While still hard to say where exactly the digital identity journey will lead, we think there are three likely scenarios for ultimate end states.

A new role

The next phase in the evolution of digital identity will be, in our view, characterized by continued maturation and consolidation, and largely driven by the forces mentioned in the previous chapter.

As platforms evolve, we think we will see a need for new products and services to cater for digital identity needs. These could be provided by existing organizations or by new entities building new types of businesses.

For example, there will be an increasing need for services around managing – and in certain cases, creating – digital identities. We can therefore see the rise of **identity providers** as a distinct entity.

Such services will likely require a certain level of official recognition. As part of GOV.UK Verify[3], for example, the UK government certifies private companies to act as identity verifiers for access to government services. These providers do the initial work of on-boarding people into the system, including collecting, verifying and safeguarding their data according to established standards. Once a person has registered with an identity provider, he or she can use that identity to access a variety of products and services, and can rely on the provider to manage the data. We see this as a model for the types of services that identity providers may provide, on a larger scale, in the future.

Identity providers will likely rely on the services of various **identity attesters** to verify information. An identity attester is an authority of some kind that confirms that a certain identity attribute is true. A bank can attest that you have an account, a government that you are a citizen, a city council that you live there, the local swimming club that you are a member.

We think attestation will become increasingly important but that the value of such attestations will vary. A credit rating attested to by an established bank like UBS may be more valuable than an attestation of creditworthiness from a social media site. As attestation becomes more important and more broadly used, it will be increasingly in demand. We can imagine specialist firms arising to provide it, or existing trusted sources – banks, for instance – adding attestation as a service. This could in turn lead to a marketplace in which attesters compete with each other, with the competition furthering technological progress.

We can also foresee a number of specialist ancillary identity services. For example, we might see the rise of **identity brokers** that assist users in managing their identities, perhaps by helping them aggregate their identity data and use it in different contexts. Such brokers might also help protect users of identity by keeping up-to-date details of reliable identity attesters. Furthermore, such brokers may become the makers of identity marketplaces.

We may also see various kinds of **identity evaluators** that provide overall identity ratings for individuals based on their personal data, as credit bureaus do now for creditworthiness. We are also likely to see the rise of **identity insurance** offerings, either protecting users from damage due to lost or stolen identity data, or protecting us from the liability associated with data breaches or system failure. Related to this will be the increasing importance of **identity safeguarders**, which will help users to safely store and if necessary recover identity data.

3 "GOV.UK Verify Guidance – as of 2 November 2016"

Home at last

As identity platforms mature and consolidate, and new roles come into being to serve specific digital identity needs, we will move towards the creation of large-scale identity platforms. In our opinion, the logical outcome of this journey is a relatively small set of regional platforms that will serve as the base identity layer for the digital economy. Like the Internet, this could also conceivably become a global platform.

What would a final digital identity platform look like? From our vantage point today it is hard to say. But observing current trends and extrapolating from experience with other technologies, we think it reasonable to expect one – or perhaps a mix – of three basic scenarios.

Government-based identity. In the first scenario, governments assume the role of universal identity provider. They own and operate the base identity layer, issue identities, verify attributes, and provide the keys for identity use. Such centralized systems offer advantages in terms of standardization and interoperability. They also offer the advantage of a single, trusted identity authority. But centralized systems also have disadvantages. They are single points of failure, single targets to attack, and single sources of potential abuse. Large, centralized systems are also not known for their ability to innovate and evolve, and some governments are more trusted than others to act in the best interests of their electorates, or in fact, their subjects.

Consortia-based identity. We might instead see a hybrid scenario in which consortia of commercial entities, working with government, provide the identity layer as part of a closed, highly regulated system. This is analogous to what we see happening in the UK, Canada and the Nordic region. A hybrid offers the advantage of a mix of public oversight and private enterprise. It gives users choice, and utilizes the forces of competition to help drive innovation and control costs. In such a setup, existing identity providers, like banks or social media companies, could more easily be incorporated. On the other hand, as it involves a larger number of independent entities than a fully centralized approach, such a system is inherently more complex, raising issues of interoperability and trust. It is also possible that different consortia could allow communication in a more federated model.

Self-sovereign identity. The two scenarios above can be seen as logical conclusions of the trends we have been discussing, and involve the provision of identity by outside entities. It is possible, however, to conceive of a completely different approach, one in which individuals own and control all of their own identity data.

In such a self-sovereign identity platform, the individual takes on the role of identity provider, collecting all of his or her available attestations and attributes, and keeping them in a digital vault or other system (similar to the way we keep our passports and birth certificates at home in safe places). We already have technology and techniques that could make such systems viable, for example, UBS Safe. Through cryptographic means, for example, we can safely store and share attestations while ensuring that they can't be falsified or misused.

We believe such a solution holds much promise. It offers optimal levels of privacy and security, and, as long as the surrounding ecosystem is geared towards it, would offer individuals almost complete control over their identity data and personas. Such a decentralized system may also be the only solution to stand up to the long term stresses to which any global and increasingly complex identity system is likely to be subjected.

There are downsides as well. In a world where you own all the proofs of your identity, losing your password would be much more than just an inconvenience. But third parties, like those outlined above, could offer services to help mitigate such risks. As such, we think self-sovereign solutions are likely to be the standard against which other platforms will need to be held.

Challenges and risks

While we believe strongly that fully digital identity platforms must – and will – evolve, there will no doubt be challenges. From security to governance to societal acceptance, we can expect many bumps along the road.

Having discussed possible paths to a digital identity future, in this chapter we take a look at some of the challenges.

Bugs

Many of these risks and challenges will be technical in nature. Among the most important:

Security. Of all the challenges facing digital identity, security is probably the most obvious, and maybe the most pressing. Today, our digital identities are anything but secure. We have had major data breaches, from Ashley Madison to Target to the recent reports over 500 million customers' data potentially being stolen from Yahoo. Such breaches are far more than just a nuisance. They are also costly. The UK, for example, loses GBP 193 billion a year to identity theft[4]. Identity hacking is also becoming part of the growing arsenal of cyber weapons, with hackers leaking stolen identities as a way to compromise their adversaries.

If we are to have a truly digital economy, we must find ways of making digital identities secure. The flip side of this is that strong security capabilities, including around identity, will increasingly become a differentiator, as well as a business. For example, we can expect a growing need for managing and securing passwords, and a growing willingness to pay for the service.

Survivability. One extremely important aspect of anything digital is what happens as technology evolves. This is particularly important in the realm of digital identity. It is one thing if we can no longer open the WordStar document containing the college thesis we wrote thirty years ago. It is another if our critical identity information gets stranded in older, inaccessible data formats.

We have a similar problem if an organization that holds key identity data goes out of business. When Lehmann Brothers failed in 2008 billions of dollars' worth of transactions became lost or stranded. It's not hard to imagine something similar happening to people's digital identities. In the same vein, how can we preserve our identity data after death? Here too, we may need the services of third parties to look after our information and keep it accessible for our heirs, if at all desirable.

Fragmentation. We believe that a lack of agreement on technologies and platforms, as well as conflicts of interest to collaborate, is a risk to the development of functional digital identity systems. We understand the need for private enterprise and initiative in working our way to any new technological platform. But there is always the danger that, as people create and implement their own solutions, we move to mass fragmentation, with this hindering progress. In such fundamental, broad-based areas as identity we feel it is much better for all stakeholders to agree on the big picture first, and to work towards this common vision.

De facto standards. Related to the above, there is the risk that one or several entities, perhaps private companies, will develop a solution which, while perhaps not ideal, becomes for reasons of convenience or cost extremely widely used. This could usher in a de facto identity standard potentially owned by a single entity. There would be no guarantee that such a platform would provide all the features, and safeguards, we would like, especially if there are not sufficient economic incentives to do so.

Technological standards. To get to a functioning digital identity solution, as with any large-scale technological development, we will need to solve the questions of technological standards and governance. That means deciding on the base standards, the underlying protocols, and the underlying oversight, as we see today with HTML, TCP/IP or ICANN. This, of course, is possible. But with so much riding on the outcome, we suspect the agreement process will be time-intensive and multifaceted.

4 "Annual Fraud Indicator 2016" © Experian Ltd and PKF Littlejohn LLP. Published in May 2016.

"Shared digital identity is a precondition for secure, efficient, digital delivery of financial, government and other services to consumers around the world. Financial regulation such as Open Banking and Payment Services Directive 2, which require financial institutions to provide access through Application Programming Interface (API) to third parties will further accentuate the need for financial services and third parties to be able to rely on a trusted source of consumer and business identity. Given the financial industry's challenges with implementing Know Your Client (KYC) solutions to comply with Financial crime regulations, this imminent challenge is not one to be taken lightly."

Ajit Tripathi, PwC
Future of Finance Forum participant

Who's in charge?

There are also a number of important governance challenges that are not technical in nature. It is worthwhile considering the most significant:

Self-sovereign versus organizational governance. We think the question of who ultimately owns and controls our digital identities will be one of the major underlying issues in the development of digital identity platforms. Above we spoke of the possibility of self-sovereign solutions, in which the individual holds their own identity data and has full control over its use. We already see the technology evolving that could enable such solutions, but will such solutions be politically or socially acceptable? Or will we instead prefer more traditional solutions, in which organizations of some kind, like governments, are the ultimate providers and holders of our identities?

Legal framework. There is currently no digital identity code of law, but for a digital economy there will need to be. There are for example major issues of liability: who is liable for data lost in a breach? Will the cost of identity liability force companies to shy away from holding customer data?

In an increasingly digital economy more of our transactions will become automated, helped by the rise of new technologies like the blockchain and smart contracts.

While not a strictly identity issue, with automation we will need to settle questions of algorithmic versus human governance. We have seen some of the problems of algorithmic governance recently (for instance with the Ethereum DAO). In any contractual situation, issues of identity will play a key role. Similarly, they may open up new business opportunities, for example for providers of identity insurance.

Regulatory issues. Connected to legal there will be many regulatory issues surrounding digital identity. One concern is that regulation takes a fragmented path, with different approaches in different jurisdictions. We already see this to a certain extent, with GDPR strengthening identity controls in the EU in ways not seen in other jurisdictions. Another danger, as in any emerging technological platform, is well-meant but ineffective or counter-productive regulation. Regulators will need to be aware of the technology and its ramifications, and may need to intervene to structure or re-structure proceedings.

High society

Finally, there will likely be, in our opinion, many societal challenges to address. The most prominent include:

Education. While perhaps not obvious, we think education is a major challenge in digital identity, and getting this right could be a major catalyst towards an inclusive, sustainable solution. Today the general public could, and perhaps should, be better informed of issues related to identity. We think banks and other financial services providers could take on this challenge. We believe there is a growing and pressing need to educate consumers about what digital identity means and what is happening with their data. Industry leaders and decision makers could also enhance their understanding of how digital identity fits into their value chains and business models. And as mentioned, regulators, along with politicians, need to maintain awareness here too, and orient their policies accordingly.

Fear and uncertainty. To the extent people are aware of digital identity issues, there is often fear and confusion surrounding them. Victims of identity theft, people concerned about collection of personal data by private companies, those who fear centralized (national or global) identity systems leading to 'big brother' scenarios – all these groups have concerns which need to be addressed. Such fears can get in the way of progress.

We may also see different groups looking at digital identity in different ways. Older generations will perhaps be more hesitant to commit their personal information to a broad-based identity platform, while digital natives may be more willing. Perhaps such trends will have an effect on how people approach privacy and identity issues in the future.

Acceptance and adoption. Finally, we think there may be significant challenges in terms of consumer acceptance of digital identity solutions. This is likely to be the case if using a new solution is less intuitive, less convenient or more expensive than the way things are handled now. Acceptance will require not just a better underlying system, therefore, but a better end-to-end user experience. Given the choice, consumers may well opt for simplicity over security and safety, which could harm identity in the long term. We think that a truly safe and secure platform will also have to offer a superior user experience for it to be widely adopted by all aspects of the economy – as we should not play down the commercial and reputational risks of a digital identity platform failure.

"The future will almost certainly be shaped by digital infrastructures supporting highly decentralized and ephemeral exchanges based on technologically mediated trust. This presupposes some working solution to the complex issue of distributed digital identity. Addressing the digital identity problem will also enable new types of innovations in the service relationships between people and service providers, as well as in person-to-person interaction."

Carsten Sørensen,
London School of Economics and Political Science
Future of Finance Forum participant

Highly qualified

Identity is not just about who we are but also about what we are capable of doing – not just about our core identity (name, address), but also relevant attributes associated with it. When it comes to such attributes and personas, digital identity solutions could add security and convenience to our current system.

Take for instance the case of qualified investors (QI). In many jurisdictions around the world regulations require that only those investors who meet certain criteria – for instance in terms of their income, net worth or professional experience – are allowed to invest in certain kinds of alternative investments, like hedge funds or private equity. This is to protect the interests of average investors who may not have the knowledge to truly understand these investments or the risks they entail.

Today it is generally the responsibility of the issuer to verify that an investor is qualified, usually by requiring the investor to produce proofs of income, wealth or experience. That requires the investor to gather and provide documentation, and the issuer to verify it. The process has to be repeated laboriously.

Imagine instead a scenario in which an investment authority of some type, for instance the Securities and Exchange Commission (SEC) in the US, takes on the role of verifying an investor's credentials and issuing a digitally assigned "Qualified Investor" attribute.

The investor could produce this credential to any issuer that requires it; this would reduce costs for alternative investments and increase their ease of use. If the issuing authority had a means to keep the credentials up-to-date, perhaps by requiring investors to re-accredit themselves on a yearly basis, then it would be convenient to ensure accurate compliance at all times.

Since such a process would likely increase security in the system and give the regulator a better picture of the investor and issuing communities. A body like the SEC may therefore see it as a natural progression of its remit to undertake this type of verification role.

Financial Services and identity

Verifying and safeguarding identity has always been a core part of banking. We believe banks have the experience, expertise and infrastructure to help shape an open, cost-effective and widely accessible future platform for digital identity.

A role to play

Developing a broad-based digital identity platform to serve as the identity layer of the digital economy will be a collective effort, involving the private sector, government, regulators, academia and others. We believe that with their experience and know-how banks have a unique perspective on the issues involved – and can play a key role in expediting the development of the solution.

For one, banks already play an important part in providing identity to the economy as holders of accounts and enablers of transactions. We know how to on-board people, institutions and assets onto digital systems. We have a great deal of experience in the highest standards of identity verification, both in our own interest and as a result of the stringent Know Your Customer, anti-money laundering and other identity regulations to which we must adhere. As a result, bank identity provision is already sophisticated and highly trusted.

Since we also safeguard wealth, which in today's world means safeguarding data, we are experts in digital data protection. This is why, despite some recent hacking, banking systems are often considered among the most secure in the world. As it is part of our function to facilitate transactions with other institutions, we have a great deal of experience building and maintaining complex, secure, and globally operating identity-based networks as well.

This is not to say that we think banks should be the sole providers of identity platforms; quite the contrary. But as we work towards a digital identity future, banks can supply their expertise and infrastructure. We think that banks are also in a position to take on a number of roles in a digital economy, for example as identity attesters or identity safeguarders, that go beyond traditional financial services.

Looking ahead

We think our experience in identity issues means we can also contribute to the discussions around setting the digital identity agenda. So what do we at UBS think the digital identity future should look like?

Our ideal platform – whether it is a single, universal platform or a collection of broad-based ones – is one that prioritizes security. It is a system in which it is difficult if not impossible to steal identities and then misuse them. It is also a system that protects individuals' privacy, providing them a great deal of choice as to what they reveal about themselves and what to keep private.

To accomplish this our future identity platform accommodates the various layers of identity we have been discussing, from our core identities to all our different attributes. By doing so, it allows us to easily use different personas in different contexts.

To allow us to share our attributes easily, this platform is highly interoperable. It is not dependent on a single, proprietary technology, but works on all the different channels that people use now or may use in the future – whether at home or on the road, whether domestically or abroad. We think it extremely important that the platform is highly inclusive as well, accessible to all no matter where they live.

While parts of the platform may have evolved through the work of private entities to solve specific identity problems, in its mature state our platform is not owned by any single company or organization. Instead it is open source and free for all to use – as the Internet is today. It is underpinned by clear identity laws and regulations that are harmonized across the world, so that all users have certainty about identity responsibilities and liabilities.

Our system also does not depend on one source of identity attestation, for instance a government. Instead it relies on a clear network of identity providers, from governments to banks to social networks, each of which provide a piece of the puzzle.

We are therefore proponents of the "self-sovereign" approach to identity mentioned previously. That means that all the pieces of the identity puzzle ultimately reside with us as individuals. As owners of our identities, we have full control – within the prevailing laws – of how our

identities are used, with the system structured by incumbent organizations such as our own.

Finally, our system is intuitive, easier to manage and use than the systems we have now. It allows us to more easily access a wider range of services, and brings us both increased convenience as well as peace of mind that our identities are secure and useful.

Home cooking

There will of course be a long way to go before we get to a solution. But we and our peers in the financial industry are already taking steps forwards.

At UBS we are looking at ways to make it easier to share identities within financial services, so that if you have been successfully on-boarded at our bank, you can use your UBS credentials to quickly open a relationship with another.

We are also looking into how identity systems might make it easier to benefit from your wealth. By more closely yet securely binding your bank account to your phone, for example, we could allow for automatic payments based on where you are, without the need for you to do anything – for instance when you drive through a toll booth.

Longer term we are looking at ways to better develop standard identity registers which can be used in automated processes like smart contracts. Another promising line of work involves helping clients better make use of the information that has been gathered about them from other sources. Such a service could allow you to more easily see what information social media sites or search engines have collected about you, and use this information for your own ends.

In short, UBS, like some of our peers, is committed to a leading role in this theme. To reassure and guide those for whom we provide services as well as society at large, we are dedicated to defining, resolving and benefitting from the challenges and opportunities we have outlined.

"Self-sovereign identity is the ultimate destination for the digital identity ecosystem. The technology is finally here to deliver the identity layer for the Internet. Self-sovereign identity will catalyze innovation on a scale never previously seen, reducing signup and purchase friction to near zero, resolving consent problems, enhancing privacy, and enabling new services to grow without the overhead of managing and protecting gigabytes of customer data."

Andy Tobin, Evernym
Future of Finance Forum participant

Afterword

This white paper has offered an insight on an important aspect of the fourth industrial revolution.

Getting digital identity right is key to a properly functioning digital economy – and we believe that banks have the responsibility and capability to progress this discussion, and perhaps define the solution.

What this solution will look like is very much in the open. Nevertheless, we are confident that it has to be secure, interoperable, scalable and inclusive.

Through harnessing the potential of biometrics, geo-spatial applications, the blockchain and AI, we can develop a solution that is, technically-speaking, everything it needs to be.

We are also confident that with the right level of commitment and collaboration, the journey towards a digital identity solution is practically possible, economically viable and politically palatable. Furthermore, we believe there is an opportunity to create a new digital market for identities that does not exist today.

UBS does not see the solution arriving as a "big bang"; we believe it will be an iterative process. This is not to say this journey has to be fragmented; we think we should guard against this. While progression is likely to be staged, these stages can and should be aligned towards a commonly agreed end-state. With so much riding on a functioning and mutually-beneficial solution, we should invest in starting out in the right way.

Definition of the problems and challenges, and an in-depth scoping of a solution is a sensible place to start. We should be mindful of the challenges and risks – and opportunities – outlined in this paper, and respectful that there are many stakeholders who would like and will require a seat at the table.

Given digital identity is not just about recording who we are – it has much more scope and potential – UBS is engaged and open to collaborate with others who have a role to play.

This is the rationale of the UBS Future of Finance Forums and white papers. At these events, and through the corresponding white papers, we bring together leaders and experts from around the world to look at how the fourth industrial revolution may play out in general, and financial services in particular.

We hope you have found this paper useful, and would be delighted to continue the discussion.

Acknowledgements

To produce this and our other Future of Finance Forum white papers, UBS is committed to collaborating with leaders and experts from across the fintech ecosystem in each of the respective themes. For this white paper, we would like to acknowledge the contribution of those below at the UBS Future of Finance Forum on digital identity in London in September 2016.

Kristian Alsing
Deloitte

Alex Batlin
BNY Mellon

Alok Bhargava
Cambridge Blockchain

Jan Camenisch
IBM

Hans-Wilhelm Dünn
Cyber-Sicherheitsrat Deutschland

Imran Gulamhuseinwala
EY

Neil Hadley
UBS

Thomas Hardjono
MIT

Martin Hartenstein
UBS

Rouven Heck
Consensys

Peter Hofmann
Swisscom

Hyder Jaffrey
UBS

Andrei Kirilenko
Imperial College London

Tim Llewellynn
nViso

Carl Massa
UK Government Digital Service

Anna Mazzone
Aravo

Jesse McWaters
World Economic Forum

Richard Morton
UBS

Stephan Murer
UBS

Eric Padua
UBS

Steve Pannifer
Consult Hyperion

Richard Peers
Microsoft

Andreas Przewloka
UBS

Steve Pulley
Thomson Reuters

Livia Ralph
UK Government Digital Service

Matteo Rizzi
Omidyar Network

Timothy Ruff
Evernym

Paul Simmonds
Global Identity Foundation

Carsten Sorensen
LSE

Patrick Spens
PwC

Kasper Sylvest
Danske Bank

Andy Tobin
Evernym

Alessandro Tonchia
smartKYC

Ajit Tripathi
PwC

Ameya Upadhyay
Omidyar Network

Eric van der Kleij
Kickstart Accelerator

Roland van der Vorst
FreedomLab

James Varga
The ID Co.

Gene Vayngrib
Tradle

Jim Vasiliou
UBS