BLOCKCHAIN AND DIGITAL IDENTITY

a thematic report prepared by

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM

EUBlockchain
Observatory and Forum

An initiative of the

European
Commission

About this report

The European Union Blockchain Observatory & Forum has set as one of its objectives the analysis of and reporting on a wide range of important blockchain themes, driven by the priorities of the European Commission and based on input from its Working Groups and other stakeholders. As part of this it will publish a series of thematic reports on selected blockchain-related topics. The objective of these thematic reports is to provide a concise, easily readable overview and exploration of each theme suitable for the general public. The input of a number of different stakeholders and sources is considered for each report. For this paper, these include:

- Members of the Observatory & Forum's Working Groups.
- "Government services and digital identity" by Dr Allan Third, Dr Kevin Quick, Mrs Michelle Bachler and Prof. John Domingue – an academic research paper prepared by the Knowledge Media Institute of the Open University, an academic partner of the EU Blockchain Observatory & Forum.
- Input from participants at the "Blockchain and e-identity" workshop held in Brussels on 7 November 2018.
- Input from the Secretariat of the EU Blockchain Observatory & Forum (which includes members of the DG CONNECT of the European Commission and members of ConsenSys).

CREDITS

This report has been produced by ConsenSys AG on behalf of the European Union Blockchain Observatory & Forum.

Written by: Tom Lyons, Ludovic Courcelas, Ken Timsit
Thematic Report Series Editor: Tom Lyons
Workshop moderator: Susan Poole
Report design: Benjamin Calméjane

v1.0 - Published on 2 May 2019.

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ACKNOWLEDGEMENTS

The authors would like to expressly acknowledge the following for their direct contributions and feedback to this paper:

Observatory Working Group Members:

- Ivona Skultétyová
- Philipp Sandner
- Daniël Du Seuil
- Konstantinos Votis
- Jolanda ter Maten
- Javier Sebastian Cermeño
- David Suomalainen
- Leïla Nassiri-Jamet

Reviewers:

- Pelle Braendgaard
- Julian Hosp
- Jamie Burke
- Christian Lundkvist
- Oscar Burgos

Identity Workshop Panelists:

- Oliver Terbu
- Rouven Heck
- Carlos Pastor
- Luca Boldrin
- Patrick Curry
- Ronny Bjones
- Kai Wagner
- Elizabeth Renieris
- Catherine Mulligan
- Hitesh Tewari
- William Skannerup

NOTE

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this paper.

Contents

Executive summary

There are few things more central to a functioning society and economy than identity. Without a way to identify each other and our possessions we would hardly be able to build large nations or create global markets. **Unfortunately, there are persistent – and increasingly serious – problems with the way digital identity works.** For historical and other reasons, the digital identity experience today is fragmented, with few standards or interoperability, and it is insecure, as the almost daily reports of hacks and data breaches reminds us. For individuals, but also for businesses and governments, the status quo is becoming less and less tenable.

Many see the problem in the haphazard evolution and “centralised” nature of the current digital identity framework. Centralised here does not mean that there is one, central source for digital identities, but rather that digital identities are almost always provided by some third-party authority (often a private company) for a specific purpose of its own. The identity information is “centralised” within that entity.

Thanks to a combination of technological advances, including the increasing sophistication of smartphones, advances in cryptography and the advent of the blockchain, **it is now possible to build new identity frameworks based on the concept of decentralised identities – potentially including an interesting subset of decentralised identity known as self-sovereign identity (SSI)**. Explaining what these concepts are, and how they might work in the European context, is the subject we address in this paper.

We start by defining exactly what identity is in an online context, showing that our digital identity is not a single thing, but rather the sum total of all the attributes that exist about us in the digital realm – a constantly growing and evolving collection of data points.

Under the current digital identity framework, these data are generally under the control of entities external to the individual they refer to. **In the decentralised identity paradigm, the idea is to put the user at the centre of the framework and so remove the need for these third parties. In this world, the user “creates” his or her own identity, generally by creating his or her own unique identifier (or a number of them), and then attaching identity information to that identifier. By associating verifiable credentials from recognised authorities, for**

EXECUTIVE SUMMARY

instance governments, users can in effect create the digital equivalents of physical world credentials like national IDs and driving licences. Since these are digital, they will, however, be more flexible and easier to manage than their physical counterparts.

By setting up a system in which the user controls not just the identity but also the data associated with it, we can create what are known as self-sovereign identities (SSI). **In an SSI approach, the user has both a means of generating and controlling unique identifiers as well as some facility to store identity data.** Users are then free to make use of whatever identity data they like. These could be verifiable credentials, but could also be data from a social media account, a history of transactions on an e-commerce site, or attestations from friends or colleagues. There really is no limit.

This ability to collect and make use of identity from a broad set of sources can help users create rich and varied sets of digital identities for themselves. It also allows them much finer control than they have today over what personal information they share in which contexts. It could even open the door to new business models, potentially allowing users to monetise their personal data should they wish to do so.

While these are intriguing ideas, making them work will be a daunting technological challenge. **We take a high-level look at what would be necessary to implement a decentralised identity framework. This includes mechanisms to allow individuals to create their own identities, often referred to as Decentralised Identifiers (DIDs), as well as means to store personal data, for example in personal data lockers or identity hubs.** We will also need digital "wallets" or other user agents to allow people to manage and use their identities.

While blockchain is not required for decentralised identity, it can be a powerful solution for different aspects of the decentralised identify framework. This includes supporting the creation and registering of DIDs, notarising credentials, providing a decentralised infrastructure for access control and data use consent, and potentially linking credentials to smart contracts to, for example, trigger automatic payments. To illustrate how this might work, we describe a number of "scenarios" as well as present a case study of how blockchain may be used in digital identity.

We then take a look at the European regulatory landscape as it pertains to digital identity. **Perhaps the most important regulation dealing**

EXECUTIVE SUMMARY

with identity in the EU is the electronic IDentification, Authentication and Trust Services regulation (eIDAS). This regulation will have a deep impact on the decentralised identity framework, above all as it pertains to government-issued/recognised identity credentials, and so we take a closer look at it.

We also examine how eIDAS touches identity on the blockchain. As fully digital ledgers, blockchains are by definition electronic documents under eIDAS. That means that blockchains, or more properly the data, including smart contracts, contained in them, cannot be denied legal force, at least not solely because of their electronic nature. Blockchains, we find, might also be useful for timestamping in an eIDAS-conform way, and we ask if perhaps blockchain-based transactions can be considered to be digitally signed under eIDAS (and if so, under what level of signature).

Our exploration ends with a few thoughts on what policy makers might do to foster the decentralised identity landscape in Europe. Chief among these is to clarify the open regulatory questions, in particular around the standing of blockchain-based signatures and timestamps under eIDAS. We also think the EU could help bootstrap the decentralised digital identity framework though educating government agencies and encouraging them to get involved in building it out, for example as issuers of verifiable credentials.

That Europe is looking seriously at decentralised identity and SSI, through for example the work on the European Blockchain Services Infrastructure, is, we think, a good sign that these concepts are taking hold in the Union. That bodes well for a more usable, secure and fair digital identity future.

Introduction: Digital identity and its discontents

WHAT IS WRONG WITH DIGITAL IDENTITY TODAY?

There are few things more central to a functioning society and economy than identity. Without a way to identify each other and our possessions we would hardly be able to build large nations or create global markets.

Yet the larger and more complex a society or market is, the more difficult identity becomes. In the physical world, we have developed various ways to deal with this, usually involving some kind of “proof” of identity claims, from wax seals and letters of introduction in pre-industrial times to the passports, driving licences and diplomas we are familiar with today.

To create a digital economy, we need to have similar kinds of proofs, or “credentials”, in the digital world. These too have been developed over the years, starting with simple digital representations of our physical, paper-based documents and moving on to more sophisticated means of digital identification like digital certificates, e-signatures, private/public key cryptography and hashing – methods that can help uniquely identify a piece of digital data (for example a digital document) and “prove” ownership of it.

Despite these useful building blocks, there are persistent – and increasingly serious – problems with the way digital identity works today. Most of these problems are not related to technology, but to processes.

One problem is that the current digital identity landscape is extremely fragmented. Surfing the web requires users to juggle all the different identities associated with their usernames or other aliases, most of which are not strongly related to their real identities. This experience is not fluid nor, unless there is a partnership between them, is there any standard way to use the data generated by one platform on another. In an ideal world, users could directly add the latest music videos viewed on YouTube to their Spotify playlists without using an external service, by connecting only once, all the while maintaining control of their data. We are far from such an ideal.

INTRODUCTION: DIGITAL IDENTITY AND ITS DISCONTENTS

Another serious problem is that identity-related data is not secure. We have become accustomed to the almost daily notices of data breaches revealing sensitive user data en masse to hackers and criminals, to the ease with which scammers can create fraudulent identities and use them to commit theft, including stealing identities from others, and to the complete lack of control we have over our personal data – data that we, knowingly or unknowingly, create when we are online, and which can be and is used to profile us, earn money on us, and potentially influence our opinions.

Nor is it only individuals who struggle with the shortcomings of the current digital identity regime. Businesses are faced with massive cost and complexity, not to mention regulatory and other risks, in both trying to secure and protect user data and in verifying the identities of the counterparties they deal with online, whether they be customers, suppliers, partners or competitors.

Governments too have reason to wish for improvements in the way digital identity is handled. Whether to correctly identify citizens in order to provide them with government-issued/recognised credentials (who is a citizen, who not), to correctly disburse benefits, to make possible electronic voting, or to combat crimes like terrorist financing or money laundering, governments rely heavily on digital identities. They will want these to be reliable. As custodians of the well-being of their citizens, businesses, markets and economies, they also have an interest in ensuring society has access to a viable, easy-to-use digital identity framework.

A third problem is that under the current identity regime there is often a weak link between digital and “offline” identities. That makes it relatively easy to create false identities. For businesses, this weak link creates fertile ground for the phenomena of false views, false “likes”, and false comments, which can help in the perpetration of fraud and lead to lost revenue. For society, this weak link facilitates the creation and dissemination of evils like “fake news”, and so poses a potential threat to the smooth running of democracy.

WHAT IS DECENTRALISED IDENTITY, AND HOW CAN IT HELP?

There are many reasons for this current state of affairs. Some of these are technical, having to do for instance with the anonymous nature of digital communications or the ease with which digital data can be duplicated or falsified.

Most of these technical problems can and are being solved, however. For many observers, the main problem with digital identity today is that it is to a great extent "centralised".

This does not mean that there is one, central source for digital identities, but rather that digital identities are almost always provided by some third-party authority (often a private company) for a specific purpose of its own. This may be because providing identity is its business, as is the case for example with certification authorities, or because it is necessary in order to provide an online service, as is the case with a bank or a social media company. Whatever the specific situation, in the current paradigm user identity information is "centralised" on the servers of the issuing entity.

Thanks to a combination of advances in hardware, including the increasing sophistication of smartphones, as well as advances in cryptography and the advent of the blockchain, it is now possible to build new identity frameworks based on the concept of decentralised identities – potentially including an interesting subset of decentralised identity known as self-sovereign identity (SSI).

In a nutshell, decentralised identities are digital identities that are created by an individual and remain under his or her control. By attaching trusted information (credentials) from authoritative sources to these identities, the individual can create trust in the claims he or she makes about his or her identity, while still maintaining that control.

How that might work in a European context, both technically and from a regulatory point of view, is the subject of the rest of this paper. We also look at the subject through the lens of blockchain technology, showing how blockchain might be employed in a future decentralised identity framework, as well as how decentralised identity can be an enabler of important blockchain use cases.

INTRODUCTION: DIGITAL IDENTITY AND ITS DISCONTENTS

As is to be expected with a new technology, there are many different philosophies and approaches to decentralised identity. Instead of picking one, we have tried to paint a broad, easily understandable picture based – as best as we could ascertain them – on the basic principles that underlie most approaches. In doing so it is possible that we have oversimplified in places, or, worse, not done justice to all viewpoints. This is of course unintentional.

It is an interesting time for the digital identity industry, a moment when many strands seem to be coming together to create something new. We believe that, in an increasingly complex world in which people increasingly mistrust data, viable, decentralised digital identities may be not just a novel technological development, but also an important one.

Towards a decentralised identity framework

HOW DO WE DEFINE DIGITAL IDENTITY?

Before we can discuss decentralised identity, it is helpful to be clear about what we mean by digital identity.[1] The question is not as straightforward as it seems.

Consider the fact that, while we all like to think we know who we are, when others identify us, they do not have access to our core sense of ourselves. Instead, they need to rely on various kinds of information that is either supplied to them or that they are able to discover – our name, for instance, or what our face looks like, or what others say about us.

In the digital identity world, a discrete piece of information attached to someone's or something's identity is referred to as an "identity attribute". There is a practically limitless potential number of such attributes.

There are for instance intrinsic "biometric" identity attributes, like our gender, what we look like, our fingerprints, our voice patterns, the way we use a keyboard or walk through a room. There are also important social identity attributes, like our name, date of birth, current address or marital status. Many of us, when thinking about identity, think in terms of "official" identity attributes given to us by our governments, like our national ID number or passport or driving licences, and these are certainly important too.

There are other social identifiers, like our family relationships, our circle of friends, our tastes in food and clothing, or our hobbies. The history of our transactions – what we have bought and sold, and how much we paid or received – is an important part of our identity too. So is the history of where we go and what we do during the day, as well as the record of what other people think of us (that is, our reputation).

The list could go on and on. The key things to remember are that digital identity is atomic in nature: based on discrete bits of information related to us. And that it can be cumulative: an identity attribute can and often is a collection of other attributes.

When we think of digital identity we therefore need to see it not as a single thing. It is rather the sum total of all the attributes that exist about us in the digital realm, a constantly growing and evolving collection of data points.

DECENTRALISED IDENTITIES – PUTTING THE USER AT THE CENTRE

In the centralised identity paradigm we discussed above, a person's identity is provided by some outside entity. In the decentralised identity paradigm we now want to explore, the goal is to put the user at the centre of the framework and so remove the need for third

[1] For the purposes of this paper, when we are talking about identity, we mean identity in a digital context. The question of what our identity is as human beings, what it means and what constitutes it is beyond the scope of this discussion.

TOWARDS A DECENTRALISED IDENTITY FRAMEWORK

parties to issue and administer identity.

This can be achieved by putting as much of the identity infrastructure as possible in the user's hands and otherwise relying on trustworthy decentralised methods, for example cryptographic algorithms that can produce mathematical proofs of the veracity of information without the need for a third-party authority.

In the decentralised identity world, users create their own digital identities. This usually starts with a user creating his or her own unique identifier or identifiers, and then attaching information to that identifier in a way that makes it possible to prove it is genuine.

Once this is done, the user can collect credentials from trusted authorities and produce them as needed.

A typical use would be for a user to collect credentials from the government, for example that he or she is a citizen, or has a certain national ID number or lives at a certain address. When it comes time to make a claim, for example that he or she has the right to vote in an election or is old enough to purchase alcohol, the user can then simply present the appropriate credential.

Thanks to various cryptographic techniques, like digital signatures, it is possible to obtain strong proof that the credential is genuine (that is, actually issued by the named authority and not tampered with since) and that the person who presents it is indeed the person being referred to.

Many people today use the term verifiable credentials (VCs) to refer to digital credentials that come with such cryptographic proofs.

Verifiable credentials play a key role in a decentralised identity framework. In essence, they are like digital versions of the physical credentials we carry around with us, such as our passports or driving licences, though with additional properties made possible by their digital nature.

There are many advantages to using decentralised identities and verifiable credentials. Not only does it give the user much more control over his or her identity, it also makes online identity much easier to use.

Once issued, a decentralised credential can be easily employed on multiple websites. Gone will be the days of constantly signing up for accounts and re-entering the same information over and over again. And if the credential changes, for instance if the user moves house, this change too need only be registered once.

Decentralised identities should also, at least in theory, be safer than centralised ones, if only for the simple reason that the user keeps the identity with him or herself. The flip side of course is that the user also assumes responsibility for the identity data. For many, the tradeoff will be worth it.

Decentralised identity is not only something to appeal to end users, however. It could also be a boon to businesses, which would no longer be solely responsible for the identity infrastructure. This can reduce both cost and risk.

That said, while the decentralised identity approach as described so far puts the user at the centre of the identity framework, it is still to a large extent reliant on data provided by third parties.

TOWARDS A DECENTRALISED IDENTITY FRAMEWORK

Digital driving licences and voter registration cards still have to be issued by a central authority. Like their physical counterparts, they remain under that authority's ultimate control (the state can issue a driving licence, and can also revoke it).

For many use cases involving decentralised identity, relying on authorities to issue verified credentials that can be associated with a user-generated identifier would not only be acceptable, it would be desirable. Today's technology, however, lets us do more.

SELF-SOVEREIGN IDENTITY – GIVING THE USER FULL CONTROL

It is possible to take decentralised identity a step further by giving users control not just of their identifiers but also of the data associated with them. This is at the heart of what is known as self-sovereign identity (SSI).

In an SSI approach, the user has both a means of generating and controlling unique identifiers as well as some facility to store identity data. This could be verifiable credentials as described above. But it could also be data from a social media account, a history of transactions on an e-commerce site, or attestations from friends or colleagues. There really is no limit to the kind of identity information that might be collected and put to use.

This in turn can open up a number of interesting new possibilities.

For instance, it can greatly expand the number and kinds of sources of identity data that can be collected. In the SSI world, anyone with a decentralised identity can issue a credential or an attestation for anyone else (though these will naturally carry different levels of trustworthiness depending on the nature of the source).

In SSI, users have much finer control over how much data they share and with whom. This makes it easy to create different digital identities for different contexts, based on different sets of credentials or identity attributes. You may have one digital identity for your healthcare provider, one for your professional networking site, and one for your social media site. Each of these would present a different "you" to the online world, and in a way that you determine.

SSI could also make it possible for individuals to monetise their personal data, for example by renting it to AI training algorithms or selling it to advertisers if they so choose. SSI can also make it easier to provide consent to third parties to use personal data and, importantly, to revoke that consent.

Last but not least, because it's a completely user-managed and controlled identity, SSI can not be taken away from a person by any authority. For many, this is its most appealing characteristic.

WHAT DO WE NEED TO IMPLEMENT DECENTRALISED IDENTITY?

There are different ways to implement decentralised identity. All approaches, however, will have to solve a similar set of problems, most of which have to do with finding ways of ensuring trust in information without recourse to some authority.

TOWARDS A DECENTRALISED IDENTITY FRAMEWORK

To get an idea of how this can work in a decentralised identity context, we can think in terms of the following basic capabilities.

- **A unique identifier**: To make a decentralised identity framework possible you need to have some basic, unique identifier that can be used in a decentralised way. These are often referred to as decentralised identifiers (DIDs). Unlike most identifiers provided by the authority issuing the identity, DIDs are created by the user (which could be a person, an organisation or even a machine). This identifier has a public part and an associated secret part, which is under the control of the person or entity that created the DID, and can be used to prove "ownership" of that DID. This is important, among other things, because it creates a strong link between the identifier and the underlying data. Important here is also the fact that a person or entity can create as many DIDs as needed for whatever purpose.
- **The actual content or data**: In a decentralised identity framework we will need to transfer data in a way that is understandable and usable by any system. This standardisation effort could take the form of verifiable credentials, where an issuer produces and signs a credential for a user that is later able to present it to a verifier. JSON and some of its specialised versions is currently the most widely used standard for identity-related data.
- **The ability to store data**: Storage is one of the core functions in relation to identity data. In a decentralised framework, credentials are usually stored directly on the user's device (e.g. smartphone, laptop) or securely held by third parties of the user's choice. Such private identity stores are variously referred to as identity hubs or personal data lockers. When solely under the control of the user, identities are considered self-sovereign. This in turn means the user can both fully control access to the data and not worry about access being revoked. Having data under the user's control also makes it more interoperable, allowing the user to employ data on multiple platforms and for different purposes, and protecting the user from being locked into one platform.
- **Appropriate security measures**: In centralised identity systems the entity providing the identity is generally responsible for the security of the identity data. In a decentralised identity framework, security becomes the responsibility of the user, who may decide to implement his or her own security measures or outsource the task to some service like a digital bank vault or a password-manager like app. While this puts an added burden and responsibility on the user, it also gives the user freedom to employ whatever security measures he or she deems fit. Decentralised identity also makes life harder for hackers, forcing them to attack data stores individually, a costly and not necessarily lucrative undertaking. (Large, centralised systems with millions of user accounts are far more appealing targets.)
- **An interface**: To implement decentralised identity, users will need a means to create and then use their DIDs. These can take the form of digital "wallets", typically on a user's phone, or other kinds of user agents. As with all other aspects of decentralised identity, the essential element here is that the wallet, and access to it, is under the user's sole control.

TOWARDS A DECENTRALISED IDENTITY FRAMEWORK

BLOCKCHAIN AND DECENTRALISED IDENTITY

While blockchain is not required for decentralised identity, it can be a powerful solution for different aspects of the decentralised identify framework. It provides a ready-made infrastructure for managing data in a decentralised but trustworthy way. This can help mitigate the use of trusted third parties or provide censorship resistance in certain circumstances.

We can imagine several potential uses for blockchain in SSI contexts, including:

- **Creation of DIDs**. Blockchain addresses make for great DIDs. These are unique, generated by the user him- or herself and already leverage public/private key cryptography.
- **Using the blockchain as a DID registry**. Blockchains could also be used as DID registries, which are databases where you store information about who is related to specific IDs and how to access information about them (server end-points).
- **Notarising credentials**. By putting their hashes on the blockchain, we can "notarise" credentials. This doesn't mean storing the credentials on the blockchain, which is generally not recommended and likely runs afoul of regulations like the GDPR. Instead it acts as a timestamp and electronic seal. This both provides proof of when the credential was created, as well as "seals" that credential by making any tampering of the credential evident to outside observers. For example, a university might send the hash of a diploma to the blockchain at the time of graduation. This provides the student with both a timestamp of when the diploma was issued as well as a way to prove at any time in the future that the diploma being presented is the one that was registered at that time.
- **Access rights and consent**. Blockchains can be used as a shared ledger to record the access rights to information. For example, a user can agree to share certain information with a social media platform but only for a limited amount of time. This consent can be recorded as a transaction on the blockchain along with its expiry date. The social media company would then have to delete the information at the expiry date and put proof of that deletion on the blockchain.
- **Facilitating smart contract execution.** In a fully integrated scheme, having links between credentials and the blockchain can allow easy smart contract interactions such as triggering on-chain payments.

Decentralised identity in action

In this section, we illustrate the potential and current uses of decentralised identity in solutions that leverage blockchain technology.

SCENARIO: ELECTRIC CAR SUBSIDY

In this example,[1] a user who buys an electric car from an electric car company wants to take advantage of a government subsidy programme for electric vehicles. The challenge is to prove to the government agency handling subsidies that the user has actually purchased an electric car and when.

Before anything else, the individual approaches the car company, which is the credential issuer for the purchase, and requests it to issue a verifiable credential associated with a DID identifying the purchaser and which confirms the purchase. This is signed by the car company and transferred to the storage chosen by the individual.

The individual then logs into the government website and informs it that he or she wants to prove they have bought this car. The government agency then sends a challenge to the user agent (wallet) asking for proof that the individual is entitled.

The user then receives a notification in his or her wallet asking if he or she wants to share this information with the agency. In this case the individual agrees.

The wallet then creates a verifiable presentation – an aggregation of verifiable credentials needed to answer the challenge. In this case the presentation is an aggregation of verifiable credentials about the individual plus the electric car company's credential tied to that individual. In addition, the individual's on-chain payment address (similar to bank information) is attached for later payment. This information is sent to the government agency, which can then be confident in the veracity of the information and also can check internally to be sure the individual has not already received a subsidy.

If all checks out, the agency issues a credential that the individual is eligible and a payment is triggered directly by a smart contract.

SCENARIO: DIPLOMAS ONLINE[2]

Educational credentials like diplomas are very important for our careers. They are also among the longer lasting of credentials, expected to be usable for a lifetime. In the physical world producing a diploma means contacting the issuing entity and going through a long and often expensive process of proving your identity, requesting an official copy of the diploma, and then waiting for it to be sent.

Issuing a diploma online as a verifiable credential can greatly streamline this process, as a digital copy of the diploma can be signed with a private key generated by the issuing entity (e.g. university) and then presented by the user when needed (e.g. during a recruitment process).

The blockchain can be used as a shared registry

[1] Note that this is a prospective scenario invented for this paper. It showcases what could exist five to ten years from now.

[2] Adapted from the W3C use case as described here.

that holds a record of valid keys used by universities. If the university changes its keys, it will register the change on the ledger, allowing verifiers to process the diploma at any point in time. This holds true even if the issuing entity is no longer in existence as the record will still exist on-chain.

CASE STUDY: KONFIDO

For a slightly more technical view, we take an example of this in action by looking at a current implementation.

Konfido is a project to create a secure and trusted paradigm for eHealth services in the EU, funded under the Horizon2020 programme.[3]

In Konfido there is a need for a privacy-preserving, cross-border exchange of health data. The challenge is to store the actions during a cross-border healthcare data exchange in an immutable and privacy-preserving way so that only involved stakeholders can search and retrieve the stored actions. To this end, blockchain is used due to its property to store logs of actions in a tamper-proof way.

In a typical transaction a doctor in Country A, say Spain, requests the Patient Summary of a Patient residing in Country B, say Denmark. The Patient Summary is returned back to the doctor. This action is then logged, and the audit log is filtered, transformed and stored in a blockchain federated network of nodes encrypted with a symmetric key.

Senders and receivers can search for the stored actions of the Blockchain network using an explorer. All the users can search for the actions, but only the sender and the receiver of the action can decrypt the logs with their private keys and read them.

In this example, we have used blockchain for digital identity in the sense of having users prove things about themselves. In this particular case, only the NCPs whose public/private key pairs match with the ones stored in the blockchain are able to decrypt and see the content of the audit logs.

[3] https://konfido-project.eu/

Decentralised identity and the European regulatory landscape

While technical developments and standards are obviously important to implementing a new digital identity framework, as with so many other aspects of technology, the legal and regulatory issues will be as important. This is certainly the case in the identity space, which touches on so many key aspects of our personal and economic lives.

While identity touches the legal and regulatory landscape in many areas, on the EU level there are two regulatory regimes that are particularly important: the General Data Protection Regulation (GDPR) and the electronic IDentification, Authentication and trust Services regulation (eIDAS).

IDENTITY AND THE GDPR

As we have described in a separate paper,[1] the General Data Protection Regulation (GDPR) lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

Since almost by definition identity information is personal data, GDPR is highly relevant for the subject of digital identity. Any large-scale identity framework will therefore have to take account of its provisions.

Depending on how it is designed, there are many areas of potential tension. An identity framework will need to work within such GDPR principles as data minimisation, purpose limitation and storage limitation. It will also have to deal with many of the rights that data subjects have under the GDPR, among them the well-known right to erasure (right to be forgotten), right of access and rights related to the automated processing of data. The GDPR also lays down clear responsibilities for data controllers and processors that will certainly need to be taken into account as well.

EIDAS: A PAN-EUROPEAN NATIONAL IDENTITY STANDARD

Perhaps the most important regulation dealing with identity in the EU is eIDAS, an EU regulation and a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.[2] This regulation will have a deep impact on the decentralised identity framework, above all as it pertains to government-issued/recognised identity credentials, and so is worth a closer look.

The eIDAS regulation was born out of the Electronic Signatures Directive of 1999, which it supersedes. That directive, which was intended to provide a legal framework for the recognition of digital signatures across the European Union, was meant to facilitate cross-border electronic transactions through the use of electronic signatures throughout the Union.

Unfortunately, for various reasons – including

[1] Blockchain and the GDPR, EU Blockchain Observatory and Forum.

[2] See Regulation (Eu) No 910/2014 Of The European Parliament And Of The Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

the fact that, as a directive and not a regulation, it left discretion over implementation into local law in the hands of Member States, leading to a fractured, non-interoperable set of standards – it fell short of its ambitions.[3] As a binding regulation, eIDAS is mandatory for Member States and so will be applied uniformly.

The purpose of eIDAS is to support the digital single market by providing a predictable legal framework to e-signatures, improving on previous legislation, and to other trust services, as well as to electronic identification. These are ancillary services crucial to digital transactions that have not been standardised on an EU level in the past. The eIDAS package includes:

- **eID**: A way for businesses and consumers to prove their identity electronically.
- **eTimestamp**: Electronic proof that a set of data existed at a specific time.
- **eSignature**: Expression in an electronic format of a natural person's agreement to the content of a document. eIDAS recognises three levels of eSIgnatures: Simple, Advanced and Qualified.
- **eSeal**: Guarantees both the origin and the integrity of a document. It is roughly the equivalent, for legal persons, of an electronic signature.
- **Qualified Web Authentication Certificate**: Ensures websites are trustworthy and reliable.
- **Electronic Registered Delivery Service**: Protects against the risk of loss, theft, damage or alterations when sending documentation.
- **Legal recognition of electronic documents**: Assurance that an electronic document can not be rejected by the court for the reason that it is electronic.

To implement this, eIDAS establishes a number of core principles binding on Member States, including the principle that Member States will cooperate on eIDs and trust services and that citizens of one Member State can use their digital IDs obtained in one country in another country to get access to government services.

Member States are free to introduce whatever means they see fit for national eIDs but once these means are notified under eIDAS, they must be accepted by all other Member States. To ensure interoperability, each Member State operates an eIDAS node, which allows for the trusted transfer of this ID Information.

The regulation also sets the framework for providing other kinds of trusted information by requiring Member States to set up lists of qualified trust service providers (TSPs) that can provide such services as verification of eSignatures and eSeals and the issuing of certificates.

This setup is intended to make things easier for EU citizens and businesses in various digital realms. It will make it much easier for EU citizens from one Member State when they move to another Member State, as they can use their already existing national ID. It will make it easier for businesses to transact with each other digitally by, for example, creating trust in electronic documents and electronic signatures on contracts. And it will add trust to the digital market in general by making it easier to identify people, organisations and documents, and for these identifications to have legal force.

[3] See "Learning from History: The Origins of eIDAS", by Marshall Nam, Docusign Blog, 9 June, 2016.

DECENTRALISED IDENTITY AND THE EUROPEAN REGULATORY LANDSCAPE

EIDAS AND BLOCKCHAIN

eIDAS touches blockchain at different levels. As fully digital ledgers, blockchains are by definition electronic documents under eIDAS. That means, among other things, that blockchains, or more properly the data, including smart contracts, contained therein, cannot be denied legal force solely because of their electronic nature.

Blockchains might also be useful for timestamping in an eIDAS-conform way. Today only trust service providers have the ability to issue timestamps that have legal force. Yet blockchains can provide a high level of trust in a timestamped piece of information. They could therefore be a way to create eIDAS-conform timestamps in a decentralised way.

Something similar happens with eSignatures and eSeals. Transactions in a blockchain are generally immutable once triggered. So the question is, can these transactions be considered to be signed under eIDAS, which is most likely the case, and if so, under what level of signature? As with the timestamp, it might be possible to consider a transaction on a blockchain to have the highest level of eSignature, that of a Qualified Signature, also in a decentralised way.

Recommendations

As we have seen, digital identity is a key prerequisite for the digital single market and hence should be a priority of policy makers. We have advocated for a decentralised identity framework in Europe. In our opinion, a decentralised identity framework in Europe could be supported in the following ways.

1. Support the role of government as an issuer of verifiable credentials.

Clearly the government can and will play an important role as an issuer of verifiable credentials. The EU could support the use of such credentials by educating and encouraging government agencies on decentralised identity and their role as issuers. The potential benefits for citizens and companies are huge, both in terms of saving costs and speeding up processes.

2. Clarify the relation of blockchains to eIDAS.

As discussed above, it is possible that blockchain timestamping and signatures could be considered eIDAS-conform, including potentially up to the highest level, by recognising blockchains within solutions managed by trust service providers. The EU could support a decentralised identity framework by clarifying these points. We feel it would position eIDAS as a powerful support for decentralised identity in Europe, aiming at having eIDAS-compliant implementations of SSI up to the highest level of assurance

3. Clarify open issues around decentralised identity and the GDPR.

We ask for clarification on the implementation requirements for GDPR compliance of various kinds of data implicated in the SSI context, such as DIDs, DID documents, revocation registries (of various implementations), public keys and addresses, and the degree to which certain kinds of obfuscation methods might take this data outside the scope of GDPR (by making it sufficiently "anonymised").

4. Clarify other potential regulatory issues.

We ask for legal clarification on the reuse of issued credentials outside of their original regulatory environments, such as for example credentials subject to the Fifth AML Directive (AMLD5), the Revised Payment Services Directive (PSD2), and eIDAS to enable horizontal comparability of credentials.

5. Continue the work of exploring a European Self-Sovereign Identity framework as part of the European Blockchain Services Infrastructure (EBSI).

As the EU develops blockchain standards under the EBSI, it should look to ensure that they are cognisant of and interoperable with DIDs and VCs.

6. Support the broad use of digital identity in cities.

Smaller cities could be an excellent testing ground for decentralised identity frameworks. The EU could support local authorities via funding and expertise to build city-wide infrastructures for their residents and so test them in a live setting.

Appendix — Who is helping shape the decentralised identity landscape?

If the above sounds complex, it is because it is. But technologically decentralised and self-sovereign identities are now more feasible than ever. To get from feasible to actual implementation is, however, a long road, and will among other things require agreement on technical standards and processes.

Right now there are many organisations, both public and private, working on such standards and so helping to build the conceptual foundation for a decentralised identity framework. In this section we bring the reader's attention to some of these organisations, most of which are good sources of more information for those readers who want to delve into the details.

- **World Wide Web Consortium (W3C)**.[1] The W3C is the main international standards organisation for the world wide web. It is working on decentralised identifiers and verifiable credentials through two working groups dedicated to these subjects.
- **Decentralised Identity Foundation (DIF)**.[2] DIF is a broad industry consortium with over 60 members founded by Microsoft, ConsenSys/uPort, Evernym and others. Its mission is to ensure the interoperability of identity platforms across blockchain networks.
- **International Organisation for Standardisation (ISO)**.[3] ISO is working on identity standards through ISO TC 307 (Blockchain and DLT)[4] and ISO SC 27 (IT security techniques).[5]
- **CEN/CENELEC**. CEN, the European Committee for Standardisation, and CENELEC, the European Committee for Electrotechnical Standardisation, are two of the three bodies (along with ETSI) that have been "officially recognised by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level."[6] CEN/CENELEC have addressed identity, among other things in a white

[1] https://www.w3.org/
[2] https://identity.foundation/
[3] https://www.iso.org/home.html
[4] https://www.iso.org/committee/6266604.html
[5] https://www.iso.org/committee/45306.html
[6] https://www.cen.eu/about/Pages/default.aspx

APPENDIX – WHO IS HELPING SHAPE THE DECENTRALISED IDENTITY LANDSCAPE

paper on recommendations for blockchain standards in Europe.[7]

- **Open-ID Foundation.[8]** The OpenID Foundation is a non-profit international standardisation organisation of individuals and companies committed to enabling, promoting and protecting OpenID technologies. Its Open-ID Connect standard is used by many applications, using JavaScript Object Notation (JSON) as a data format.
- **Internet Engineering Task Force (IETF)**.[9] The IETF is an open standards organisation, developing and promoting voluntary Internet standards, especially the standards that comprise the Internet protocol suite TCP/IP.
- **International Association of Trusted Blockchain Associations (INATBA)**.[10] INATBA, a new organisation launched in April 2019, brings together industry, startups and SMEs, policy makers, international organisations, regulators, civil society and standard-setting bodies to support blockchain and Distributed Ledger Technology (DLT) to be mainstreamed and scaled-up across multiple sectors. It's expected to play a major role in shaping how blockchain and identity will work in Europe.
- **Hyperledger Indy**.[11] Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. It has developed specifications, terminology, and design patterns for decentralized identity along with an implementation of these concepts

[7] https://www.blockchaineconomia.es/wp-content/uploads/2018/11/Libro%20blanco%20estandarización%20Bck.pdf
[8] https://openid.net/foundation/
[9] https://www.ietf.org/?gclid=EAIaIQobChMIoLvxjPSz4QIV1xXTCh3rIwhfEAAYASAAEgIjEfD_BwE
[10] https://inatba.org/
[11] https://www.hyperledger.org/projects/hyperledger-indy

Appendix – Blockchain Terminology

What is a blockchain?
Blockchain is one of the major technological breakthroughs of the past decade. A technology that allows large groups of people and organisations to reach agreement on and permanently record information without a central authority, it has been recognised as an important tool for building a fair, inclusive, secure and democratic digital economy. This has significant implications for how we think about many of our economic, social and political institutions.

How does it work?
At its core, blockchain is a shared, peer-to-peer database. While there are currently several different kinds of blockchains in existence, they share certain functional characteristics. They generally include a means for nodes on the network to communicate directly with each other. They have a mechanism for nodes on the network to propose the addition of information to the database, usually in the form of some transaction, and a consensus mechanism by which the network can validate what is the agreed-upon version of the database.

Blockchain gets its name from the fact that data is stored in groups known as blocks, and that each validated block is cryptographically sealed to the previous block, forming an ever-growing chain of data. Instead of being stored in a central location, all the nodes in the network share an identical copy of the blockchain, continuously updating it as new valid blocks are added.

What is it used for?
Blockchain is a technology that can be used to decentralise and automate processes in a large number of contexts. The attributes of blockchain allow for large numbers of individuals or entities, whether collaborators or competitors, to come to a consensus on information and immutably store it. For this reason, blockchain has been described as a "trust machine".

APPENDIX – BLOCKCHAIN TERMINOLOGY

The potential use cases for blockchain are vast. People are looking at blockchain technology to disrupt most industries, including from automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel. While blockchain is definitely not the solution for every problem, smart contract automation and disintermediation enable reduced costs, lower risks of errors and fraud and drastically improved speed and experience in many processes.

Glossary

The vocabulary used in the context of blockchains is quite specific and can be hard to understand. Here are the essential concepts you should know in order to navigate this breakthrough technology:

- **Node:** A node is a computer running specific software which allows that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network.
- **Signature:** Signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography allows someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key.
- **Transaction:** Transactions are the most granular piece of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network, a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that the transaction content has not been manipulated while being transmitted over the network.
- **Hash:** A hash is the result of a function that transforms data into a unique, fixed-length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data.
- **Block:** A block is the data structure used in blockchains to group transactions. In addition to transactions, blocks include other elements such as the hash of the previous block and a timestamp.
- **Smart contract:** Smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus leveraging the trust and security of the blockchain network. They allow users

APPENDIX – BLOCKCHAIN TERMINOLOGY

to automate business logic and therefore enhance or completely redesign business processes and services.

- **Token:** Tokens are a type of digital asset that can be tracked or transferred on a blockchain. Tokens are often used as a digital representation of assets like commodities, stocks and even physical products. Tokens are also used to incentivise actors in maintaining and securing blockchain networks.
- **Consensus algorithm:** Consensus algorithms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means depending on the specific needs. The most famous consensus algorithms include proof-of-work, proof-of-stake and proof-of-authority.
- **Validator nodes:** Validator nodes are specific nodes in a network that are responsible for constituting blocks and broadcasting these blocks with the network. To create a valid new block they have to follow the exact rules specified by the consensus algorithm.

Learn more about blockchain by watching a recording of our Ask me Anything session.