

Public-Private Governance of Blockchain Digital Identity Solutions

A whitepaper from InfoNetworks



Frank Cona and Michael Palage

Table of Contents

1. Introduction.....	3
2. Personal Information is at Risk Online.....	3
3. Evolving Approaches to Digital Identity.....	4
4. The Potential of Blockchain for Digital Identity.....	6
5. The Advantages of Digital Identity Controlled by the Individual.....	8
6. A Network-of-Networks for Digital Identity.....	9
7. Evolving Global Legal Rights Must Be Addressed.....	10
8. The Limitations of Private Governance.....	12
9. A Public-Private Governance Framework.....	14
10. Next Steps.....	15

1. Introduction

As the Internet has become a common medium for virtual every type of transaction, there is a growing risk to personal information from online transactions. This has led to a variety of new approaches to digital identity to address those risks. In particular, distributed ledger technology (“blockchain”) is being explored for creating a new paradigm for digital identity in which an individual’s personal information remains under their control and not aggregated with various service providers. Such “personal IDF” solutions provide significant data privacy advantages.

However, the use of digital identities across borders and globally creates significant legal and political challenges that must be addressed to drive adoption of this new digital identity paradigm. While private communities are driving consensus on standards for blockchain, private governance alone may not be sufficient to address these challenges. A public governance layer, independent of any one sovereign state, may be needed.

An intergovernmental agency (or community of agencies), for example, may be ideally suited to work with sovereign governments to promulgate policies, regulations, and “due process” procedures. Working at both the internationally and local level, IGO’s can ensure parties transacting with digital identities retain their ability to obtain legal redress within appropriate courts and administrative tribunals and that such policies and procedures appropriately balance differing views among sovereign governments as to data security and privacy rights. Industry standards and protocols for blockchains would be bounded only by the base requirements established under the public governance for the use of digital identity. Thus, the private sector would otherwise remain unencumbered and free to drive consensus on standards for the interoperability of blockchain solutions in an open “network-of-networks” for digital identity, and to innovate differing digital identity solutions.

2. Personal Information at Risk Online

It is difficult to overstate the global impact of the public Internet. It has transformed communications, commerce, information sharing, and the very manner by which human beings interact; and has become the common medium for virtually all types of transactions.

While the rapid pace of innovation in Internet technology has enabled an increasing amount of transactions to occur entirely online, one area that has lagged is “digital identity.” As used in this paper, *digital identity* broadly refers to any set of information used to represent some entity (a person, organization, application, or device) in an online transaction (e.g., exchanging information, purchasing a product, transferring fund, etc.) with another entity.¹ A simple form of digital identity is a password-based access credential and user profile, which are provided to verify that an entity is authorized to engage in a transaction. Digital identity can be security credentials used for machine-to-machine communication, such as with transactions among devices forming the “Internet of Things” (IoT). It can also refer to civil or national identification in digital form (i.e., a digital passport or other government-recognized form of identification).

There are three fundamental aspects of any digital identity: identity creation (i.e., attestation of identity information to create valid identity credentials), authentication (i.e., verification of those credentials), and authorization (i.e., verification of rights provided by those credentials). For example, when a user wants to access a service provider’s web site, they must first

¹ https://en.wikipedia.org/wiki/Digital_identity

demonstrate their identity to a service provider, who verifies their identity information and provides access credentials (digital identity). When the digital identity is used to access the service provider's web site, the service provider determines the access rights associated with that digital identity and authorizes the user to access portions of the site based on those rights.

Digital identities are necessary for the majority of online activity: accessing services through web sites, e-commerce transactions, communication among IoT devices, etc. Today, a user typically creates a different digital identity (e.g., a user name and password) with each service provider, and that user's personal information is then typically aggregated with that service provider—with their personal information consequently also being duplicated across multiple service providers. This aggregation and duplication of personal information creates “honeypots” of centralized personal data ripe for data breaches.²

The tremendous growth in the aggregation of personal information online using digital identities has raised significant security and privacy concerns over how identity credentials are stored and used. Password-based credentials provide ever increasing security risks, as most data breaches arise from phishing or other types of social engineering.³ Additionally, over 45% of all credit card fraud is now online in virtual (“card not presented”) transactions, with identity theft being the primary cause.⁴ Consequently, there have been numerous approaches to enhance the security of password credentials.

But password-based credentials remain susceptible to compromise (whether through social engineering or brute-force hacking) due to the need for human beings to use passwords that can be more easily recalled, or to store them in easily accessible ways. Attempts to enhance security, such as multi-factor authentication (e.g., out-of-band verification via email or text, and security questions), increases in password complexity, and regular changing of passwords compound user aggravation.

In addition, with an estimated 38 billion IoT devices online by 2020,⁵ there is a concerted effort to determine the applicable security standards for machine-to-machine communication among these devices, and to develop technologies that reduce potential breaches. While some use-specific protocols like Z-wave are ahead of the curve,⁶ general IP-based IoT devices still pose significant risks for attacks.⁷

3. Evolving Approaches to Digital Identity

In a report last year, *Digital Identity: Issue Analysis*,⁸ Consult Hyperion provide an overview of some of the various approaches to digital identity, which they illustrate on the following chart:

² <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

³ <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/takeaways-from-the-2016-verizon-data-breach-investigations-report/>

⁴ <http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>

⁵ <https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020>

⁶ <http://z-wavealliance.org/z-wave-scores-huge-ul-win-for-security-a-first-for-mesh-technology/>

⁷ <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>

⁸ http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

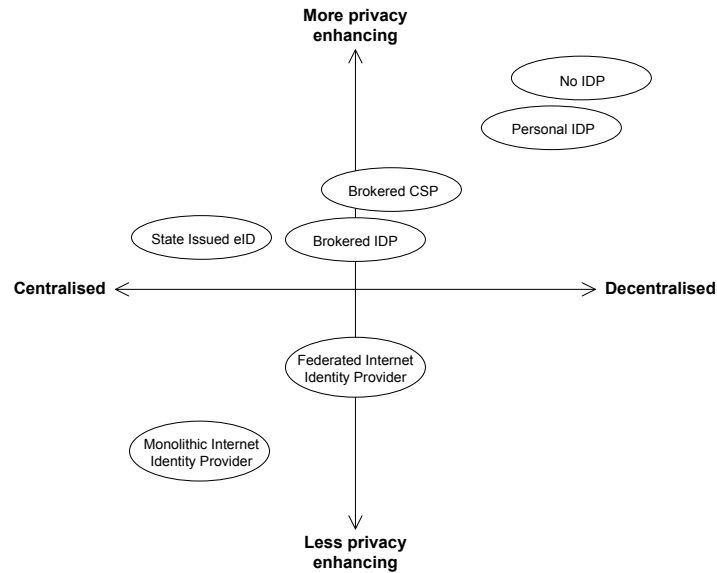


Figure 3, Positioning Architectural Models

As noted previously, different access credentials are typically created with each service provider today. The evolution of identity as a service (IDaaS), however, enables one or more aspects of digital identity (creation, authentication, or authorization) to be performed by a third-party identification provider (IDP). With IDaaS, the same digital identity may be federated for use across multiple service providers, with varying degrees of centralization of user data. This is illustrated in the above chart.

For example, some governments have implemented digital identity verification programs, under which citizens of that country register with an IDP, providing various personal information to attest to their identity. Then, whenever the government needs to authenticate and authorize their digital identity for various government services online, a request is brokered through an IDP—rather than the individual having to submit their personal information for that transaction. Examples of such systems are GOV.UK Verify⁹ in the United Kingdom, and DigID¹⁰ in the Netherlands. Other eID examples include Estonia eID,¹¹ Austrian eID,¹² and Peru eID.¹³ Other federated forms of digital identity include shared authentication schemes (such as OAuth, OpenID, OpenID Connect, and Facebook Connect).¹⁴

With such systems, an individual does not have to repeatedly provide their personal information. In addition, less personal information needs to be maintained with the IDP once the initial identity proofing has been completed, and in some systems, identity credentials for each service are decoupled to enhance security and privacy. But personal data is still aggregated in honeypots to varying degrees. And, users still need to maintain password credentials for accessing the government web sites, which are subject to the security concerns noted above.¹⁵

⁹ <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>

¹⁰ <https://www.digid.nl/en/>

¹¹ https://joinup.ec.europa.eu/node/123843?utm_source=epractice&utm_medium=epractice&utm_campaign=epractice

¹² <http://ec.europa.eu/idabc/en/document/4486/5584.html>

¹³ <http://www.cryptovision.com/wp-content/uploads/2015/06/Mindshare-2015-D2-1100G-Peru-eID.pdf>

¹⁴ https://en.wikipedia.org/wiki/Single_sign-on

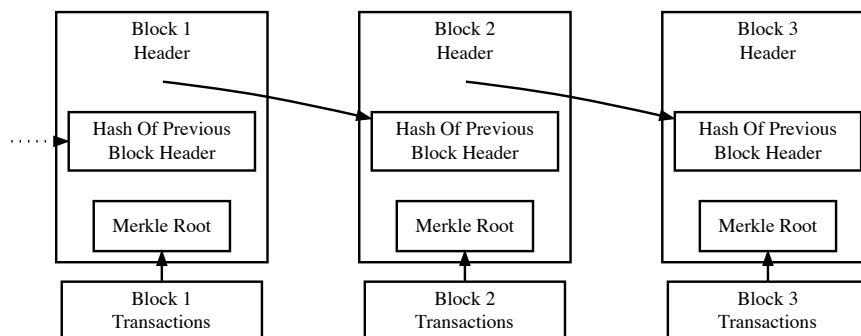
¹⁵ Although, the Netherlands indicates that it is working on a mobile application for their program that avoids the need to use password credentials (e.g., scanning a QR code and entering a PIN). <https://www.digid.nl/en/about-digid/app/>

4. The Potential of Blockchain for Digital Identity

Many organizations today are investigating distributed ledger technology (“blockchain”), for a wide variety of applications—even for the operation of the Internet itself. In particular, the need for more secure digital identity and greater privacy for personal information online has led to a significant amount of activity in investigating blockchain for digital identity. A variety of IDP’s have also emerged that are exploring uses of blockchain for federated digital identity systems.¹⁶ For example, Airbnb is experimenting with blockchain to enable users to create a digital identity profile for use with their services within their own “trusted network”, but which could also be used as digital identification for providers for related services in other trusted networks.¹⁷

Many banks and other financial service providers are also exploring blockchain technology. JP Morgan, for example, has several blockchain test projects, one example being a distributed transaction ledger that enables regulators to access and verify transaction information for compliance, while maintaining the privacy of the parties to the transaction.¹⁸ In another example, the Credit Union National Organization (CUNA), is currently involved in a blockchain pilot program called CULedger, in which blockchain technology is being tested for various applications among credit unions.¹⁹ Beyond digital identity for individuals and organizations, applications of blockchain are also being considered to verify IoT devices in a more security and privacy-enhanced manner.²⁰

Blockchain technology originated with Bitcoin, a decentralized cryptocurrency.²¹ The Bitcoin blockchain is a serial ledger of verified transactions formed by linking immutable sets (blocks) of transaction data in the order that they occurred, as illustrated in the following chart from Bitcoin.org:



Simplified Bitcoin Block Chain

The data for each transaction is grouped into a block and “hashed” with the preceding transaction in that block forming a “merkle root” for the block header, which is itself hashed with hashed block header from the previous block (which is itself a hash of the previous block’s merkle root and the hashed block header from the block before that one, all the way back to the

¹⁶ <https://letstalkpayments.com/12-companies-leveraging-blockchain-for-identification-and-authentication/>

¹⁷ <http://qz.com/657246/airbnb-just-acquired-a-team-of-bitcoin-and-blockchain-experts/>

¹⁸ <http://fortune.com/2016/10/04/jp-morgan-chase-blockchain-ethereum-quorum/>

¹⁹ <http://www.culedger.com/Pilot>

²⁰ <http://www.postscapes.com/blockchains-and-the-internet-of-things/>

²¹ <http://historyofbitcoin.org>

original “genesis” block for the chain).²² The entire validated ledger is replicated, shared, synchronized and available to every node on the network.

Each Bitcoin user has a digital wallet that contains an identifying address, a currency balance, and a private cryptographic key. When a user wants to initiate a transaction, the wallet is used to create a transaction order with data (bitcoins) to be transferred and the recipient’s address, and cryptographically “hashes” the order using the private key.

The hashed transaction order is broadcast on the network so that it can be confirmed by a group of validating nodes (“miners”) who use a “consensus” protocol to validate the transaction to add it to the chain. The consensus protocol involves computing repeated attempts to use the transaction data and a nonce (an irrelevant piece of data, like an incremented number) to generate random hash numbers to eventually produce a number below a set target. The miners are incentivized by receiving a portion of the bitcoins as fees. The hashed block from the first miner to beat the target is the one that is added to the chain. The updated chain is then synchronized across each network node as the authoritative ledger for all the transactions.

The original Bitcoin blockchain was a “permissionless” peer-to-peer network for transferring a virtual currency from any one party on the network to any other party on the network. It is permissionless because there is no trusted authority (such as a bank or clearinghouse) verifying that the transactions are legitimate and that the ledger for the entire sequence of transactions remains correct. Instead, transactions are verified by the consensus protocol. Trust is established due to the degree of difficulty established for the miners; and the increasing difficulty of corrupting a transaction recorded on the blockchain as it increases in size.

The computational demands for validating transactions in a conventional permissionless system like Bitcoin can make it inefficient. This has led to the investigation of “permissioned” networks for applications of blockchain for digital identity, in which a trusted authority manages access to the networks by users, and who is authorized to perform verification of the transactions. Permissioned blockchains can establish a consensus protocol that is not as computationally demanding but is still secure because of control over which parties are authorized to join the network. Thus, permissioned blockchain has the potential to leverage the other benefits of blockchain for more secure digital identity, where the economic incentive model of cryptocurrency is not needed. Yet, permissioned blockchain still allows for identity information to be obtained under appropriate “due process” procedures in the event of a legal dispute—which can be more challenging with permissionless systems.

Blockchain is still nascent technology, particularly for applications outside of cryptocurrency. There are challenges, such as transaction speeds, the verification process (e.g., managing trusted authorities, processing overhead), cryptographic security, and data limits that need to be addressed. And, blockchain represents a potential paradigm shift to a decentralized network for the storage and use of personal information that will require cultural adoption by industry professionals as well as users.

Nevertheless, blockchain provides some significant potential benefits for digital identity. It can enable IDaaS with limited access to personal information, and can enable more control by an entity over how their identity information is subsequently used or distributed. The redundant,

²² Hashing involves cryptographically combining multiple inputs to produce an output number. If any input is different in any way, the algorithm produces a different number that has little or no correlation to the “correct” output. Because of this, the inputs can only be determined by brute force calculations trying different potential inputs.

distributed storage of blockchain data enables it to be reliably complete, consistent, timely, accurate, and widely available. The decentralized nature of blockchain removes a central point of failure improving its ability to withstand malicious attacks. Transactions on a blockchain can be publicly viewable, creating transparency, and the records are immutable. Use of a common ledger reduces the duplication and complications of multiple data storage.²³

5. The Advantages of Digital Identity Controlled by the Individual

In their report, Consult Hyperion discuss various principles for digital identity and set forth several considerations for developing digital identity solutions:

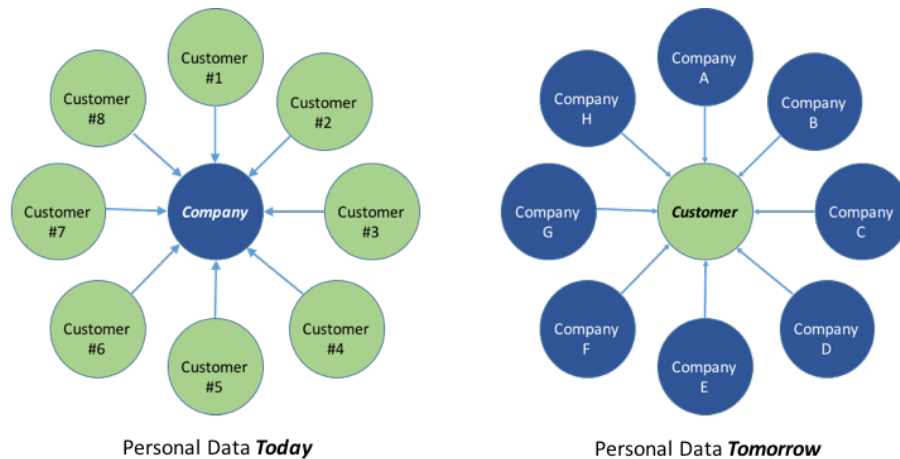
- Providing sufficient individual control over their privacy protection
- Incorporating privacy rights (beyond data security)
- Addressing identification separately from authentication and authorization
- Minimizing data exchange (such as using tokenization)
- Providing a viable commercial model that dis-incentivizes abuse of personal data
- Having an effective legal / regulatory environment
- Addressing questions of liability
- Addressing the need for mass adoption
- Addressing limits of digital identity systems and privacy rights

Based on their review, “personal IDP” / “no IDP” models (see the previous chart) using a common identity framework generally provide significant advantages from a privacy perspective over more fragmented, user-case specific approaches.

While the federated approaches previously discussed are somewhat less centralized and are more user-centric, an individual must still provide their personal information to be aggregated by service providers, and this personal information can be re-used by those providers for various purposes with less control by the individual.

But alternative approaches to digital identity are being considered in which personal data is no longer aggregated with service providers. Instead, an individual’s personal data remains under the control of the individual, and can be accessed by various providers only to the extent needed to verify the individual’s identity or credentials. This concept is illustrated below:

²³ <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html>



Under this new paradigm, an individual may create, keep, and maintain a common identity for use across many different services, rather than having to maintain multiple sets of identification credentials (e.g., passwords, or user profiles), or having to provide their personal data (and the control of that data) aggregated and re-used by each provider. A service provider may access and use the individual's identity information, but the information remains under the control of the individual, rather than being aggregated with those service providers.

For example, the Sovrin Foundation have proposed a model for “self-sovereign” identity in which users would manage and control their own identity credentials. Individuals would create a digital identity with various identity credentials on a public permissioned blockchain managed by Sovrin (a U.S. not-for-profit organization). These credentials can be accessed and verified by service providers globally as needed, but the individual's personal information remains under the control of that individual, with pointers to that data in the blockchain. In other words, they can use their digital identity across multiple service providers but their identity and personal information is not tied to any one service provider—it remains portable with them.²⁴

When developing digital identity solutions for use on a global, cross-border basis, there are tremendous advantages in security and data privacy enabled by a “personal IDF” based on permissioned blockchain. Such an approach will better adapt to the evolving requirements for privacy rights around the world (discussed in more detail below), as it will minimize the transmission and storage of personal information across borders. And, it will better adapt to agreed-upon due process requirements for resolution of disputes.

6. A Network-of-Networks for Digital Identity

As blockchain-based identity solutions emerge, there will be a growing need for standardization—for the blockchains themselves as well enabling technology used with them. Open standards and protocols will be needed to ensure interoperation among various blockchain solutions for digital identity, enabling technologies, IDP's, and service providers. Just as with the Internet itself, fostering an open “network-of-networks” for different digital identity solutions will drive adoption and enable individuals and organizations to use their provider of choice for a wider range of services and on a global basis. With an open ecosystem of different blockchain solutions, users will also benefit from competition to improve these solutions.

²⁴ <https://www.sovrin.org/docs.html>

There is already a significant amount of private community activity driving standards for blockchain technology. For example, in September 2016 the International Organization for Standardization (ISO) convened a technical committee to evaluate the standardization of blockchain and distributed ledger technologies to support interoperability and data interchange among users, applications and systems.²⁵ The ISO decision was based on a proposal by Standards Australia, who ISO appointed to lead this effort.²⁶

Based on the Australian proposal, the ISO committee will focus on permission models public and private networks, smart contracts, API's, and other key aspects of blockchain including terminology, process and method, IT privacy, cyber security, and interoperability.²⁷ In particular, the committee will leverage the existing SWIFT ISO 20222 standard for electronic data interchange between financial institutions and is widely used in the financial services sector.²⁸ W3C and other Internet community groups are also studying the standardization of blockchain and use case applications.²⁹

The focus of the ISO committee is much broader than digital identity, but it is critical that the base requirements for global digital identity are addressed in any standards that would govern blockchain and its enabling technology. As part of this, existing standards for digital identity generally should be considered with respect to standards for blockchains to ensure requirements for global digital identity using blockchain are addressed.

The FIDO (Fast Internet Online) Alliance is promulgating standards for the authentication and authorization of identity credentials (without passwords) from devices that are relevant to “wallet” applications for digital identity and for verification of identity credentials on the blockchain.³⁰ Examples of FIDO implementations include biometric fingerprint authentication adopted on smartphones by many service providers. As another example, The OpenID Foundation promulgates OpenID Connect,³¹ which is an authentication protocol based on the OAuth 2.0 family of specifications for access authorization³² based on digital identity. OpenID Connect incorporates a federated identity model, which enables IDP's to authenticate clients and devices with a persistent log-in, without the need to re-enter passwords.

As with the evolution of the Internet (itself a “network-of-networks”), private communities can drive consensus for blockchain standards that enables seamless interoperability as well as an open ecosystem that fosters innovation through free market competition.

7. Evolving Global Legal Rights Must Be Addressed

But the evolution of blockchain in the context of global digital identity poses additional challenges beyond those faced by a globalized general communication and transaction medium like the Internet. In addition to other areas of the law, the great variation in legal rights and

²⁵ http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=6266604

²⁶ <https://www.cryptocoinsnews.com/iso-appoints-australia-take-global-lead-blockchain-standards/>

²⁷ <http://www.standards.org.au/OurOrganisation/Events/Documents/Blockchain%20NFTA%20Information%20Sheet.pdf>

²⁸ https://www.iso20022.org/the_iso20022_standard.page

²⁹ <https://www.w3.org/community/blockchain/>

³⁰ <https://fidoalliance.org/specifications/overview/>

³¹ <http://openid.net/connect/fag/>

³² OAuth itself provides a standard for providers to offer their services without forcing their users to expose their identity credentials—it is directed at verifying authorization to participate in a transaction, like accessing a web site, and not identity proofing or authentication. <https://oauth.net/about/>

political world views with respect to personal information alone presents specific and significant challenges for digital identity when used on a global basis. Notably, the proposal by Standards Australia indicates that the work by the ISO technical committee will specifically exclude legal obligations and regulatory matters addressed by government jurisdictions.

When establishing conventional digital identities with service providers today, users typically agree to waive their privacy rights to differing degrees with respect to the use (and re-use) of their personal data in exchange for accessing services from those providers. Government mandated privacy rights (which can't be waived) vary significantly, however, across sovereign states—including when and how such data can be transmitted across national borders in online transactions. And, there is similar variation in individual rights with respect to the access, use, and retention of personal data by sovereign governments, as well as by other parties. This creates challenges for users in controlling the use of their personal information in both national and international transactions, challenges for third parties who have a legitimate need to obtain that personal information (such as in the event of a litigated dispute), and challenges for service providers maintaining compliance with the respective privacy laws of various sovereign states.

While there is a common concern among individuals, communities, and sovereign states as to the need for privacy, there are widely differing and continually evolving views as to the manner of protections to be afforded to personal information. The European Union, for example, has a very comprehensive regulatory framework for the use of personal information, with extensive rights given to individuals with respect to the retention and use of their personal information.³³ Compare this with other sovereignties having different cultural views toward privacy rights, such as the United States³⁴ or China.³⁵ And, some countries, like Nigeria, are adopting data protection technologies, but are still developing corresponding data protection laws.³⁶

Add to this the tremendous variation among sovereign jurisdictions as the manner and extent to which citizens can seek legal redress against private parties and/or government actors with respect to a dispute over their rights. Consider, for example, the great variation in such “due process” and the inherent rights of individuals among the United States, the European Union and European nations, the Middle-East, and in Asian countries.

The global recognition of the need for privacy rights, yet shifting and differing views within sovereign nations is explored by Consult Hyperion in their report. They note:

However, it does not follow that, because the right to privacy is central to the maintenance of a vibrant and liberal social and political order, it is a static concept. Its content and confines remain contested, subject to never-ending games of tug-of-war between individuals, governments and corporations. Innovation and change – not just in technologies, but in migration and border flows, security and conflicts, attitudes and priorities – inform and challenge our conceptions of the private and the public. The continual development of new means to undermine or protect privacy gives rise to new discussions about how to contextualise it, and new questions about its salience in changing contexts.

³³ <http://ec.europa.eu/justice/data-protection/>

³⁴ <https://theintercept.com/2015/10/06/top-european-court-rules-that-nsa-spying-makes-u-s-unsafe-for-data/>

³⁵ https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html

³⁶ <https://techpoint.ng/2016/07/15/nigerian-government-biometric-vehicle-database/>

Equally, it does not follow that the existence of constitutional protections for the right to privacy or of data protection laws in developing countries are indications that privacy is engendered and recognised as a societal good. In a number of cultures, the autonomy and functioning of the community is prioritised over the autonomy of the individual, leading some to argue that privacy may be a Western concept. On the other hand, however, a number of non-Western cultures have long traditions of protecting privacy in the context of the home and the family; the Quran, for example, contains a number of passages on the importance of privacy. South Korea is home to one of the most active Constitutional Courts in the world when it comes to privacy; the Court has recently invalidated laws which criminalise adultery and which mandate the use of real names online, on privacy grounds. (Citations omitted.)

The governance framework for the global use of digital identity solutions blockchains must ensure that parties will retain their right to legal redress against responsible parties in the appropriate sovereign courts or private tribunals. It must balance commonly accepted privacy rights internationally as well as differing rights within sovereign states and jurisdictions. The governance model also must be trusted to satisfy the respective due process rights of citizens of different sovereignties when transacting internationally, while—at the same time—precluding any sovereign government from exceeding the bounds of its sovereignty.

8. The Limitations of Private Governance

In their white papers, the Sovrin Foundation proposes that the governance for a global digital identity network be “provided by a private-sector international non-profit organisation, representative of all who have Sovrin identities, in much the same way as the Internet’s governance is overseen by ICANN.”³⁷ While we agree with Sovrin that such a network “cannot be owned or controlled by any single company, organisation, or government”, we believe that governance by a private communities alone is not an adequate framework for global digital identity systems.

There are a number of challenges for private governance with respect to global digital identity specifically. Private communities may struggle to gain legitimacy or to sufficiently accommodate differing and evolving governmental approaches to data privacy. More fundamentally, these communities may not be legally empowered to adequately address the legal and political impact of online transactions using global digital identities (highlighted previously).

For example, online transactions across jurisdictions raise a number of “conflict of law” issues:

- Contracting parties may choose the jurisdiction whose laws governing their contracts, regardless of where they, or any impacted persons or property are located
- Sovereign states are fundamentally free from control by other governments, and may disregard the a party’s choose of law in certain situations
- Sovereign states may also agree by treaty or in comity to respect, or apply, the laws of another country, which may supersede a party’s choose of law
- Sovereign states often seek to harmonize various laws among them, but the extent and manner by which some nations participate may vary

³⁷ Sovrin white paper, *The Inevitable Rise of Self-Sovereign Identity*, page 13.

- Whether a party has entered into, or performed under, a contract in “good faith” may have differing implications to resolving a dispute in different jurisdictions

Beyond the substantive laws that apply to a given legal issue, adjudication of disputes also typically requires appropriate proof of a party’s identity and their personal information, proof that the tribunal has the legal authority over a person or property at issue, and proof of any other relevant facts as to a transaction at issue. The “due process” requirements for obtaining such information and for using it as evidence before a tribunal also vary in different sovereign states, and are subject to similar conflict of law issues.

Thus, when a dispute arises across jurisdictions, the relevant tribunal (whether a sovereign court or private tribunal) must consider potentially conflicting laws to determine its authority over a person or property, what information a party has a right to access, what substantive law applies, how to apply it, etc. Such determinations can be further complicated when one of the disputing parties is a sovereign government or other public entity, particularly if it is a criminal proceeding against an individual.

These legal (and sometimes political) concerns still exist in the digital world—even with the use of “smart contracts.” That is, the automation of a digital transaction with blockchain does change the underlying due process and other legal issues that must be addressed.

The evolution of online dispute resolution (ODR) is illustrative. ODR involves the use of online communications systems for alternative dispute resolution (i.e., the resolution of disputes using private arbitrators instead of through a sovereign court or other public tribunal). The rise of the public Internet in the 1990’s gave rise to the need to adapt substantive laws that were created for the physical world to “cyberspace” as well as to adapt the processes for resolving legal disputes. Over the past several decades, there has been significant activity on both fronts, but to date, both legal and technical approaches to ODR remain limited in terms of the scope of issues with which they are used as well as the jurisdictions within which they are available.

An IUM Law Journal article from last year, *Towards an Effective Legal Framework for Online Dispute Resolution in E-Commerce Transactions: Trends, Traditions, and Transitions*, provides a good history of ODR and provides a current overview of several public and private ODR systems. While the article concludes that the “ability to resolve disputes and complaints online without the need for traditional offline contact seems to be the most effective means for providing access to justice for online consumers”, the overview provided in the article itself aptly illustrates that there is still no uniform legal framework for even the private resolution of online disputes, let alone disputes raised in sovereign tribunals).³⁸

Indeed, the challenges that the private governance of the Internet itself has faced is also illustrative. ICANN, the global coordinating body of the Internet’s unique identifiers, offers an interesting example of the strengths and weaknesses of a private sector led governance model. One of ICANN’s first successes was the implementation of the Universal Dispute Resolution Policy (UDRP). Prior to the implementation of the UDRP, trademark owners had to engage in costly litigation in jurisdictions around the globe to enforce their legal rights against largely anonymous registrants. The UDRP greatly simplified this process by permitting trademark

³⁸ https://www.researchgate.net/publication/303896528_Towards_an_Effective_Legal_Framework_for_Online_Dispute_Resolution_in_E-Commerce_Transactions_Trends_Traditions_and_Transitions

owners to file an administrative proceeding against a registrant and the domain name that they had registered with a dispute provider accredited by ICANN.³⁹

One of the original dispute providers selected by ICANN was the World Intellectual Property Organization (WIPO), a specialized agency of the United Nations, that serves as a global forum for intellectual property services, policy, information and cooperation. In implementing the UDRP, ICANN did not seek to supersede national trademark laws. Therefore, the registrant of a domain name that lost a UDRP proceeding, was provided the ability to file a timely legal action in a court of competent jurisdiction challenging the administration proceeding decision to stay enforcement of any UDRP decision. While the UDRP provides trademark owners a cost-efficient mechanism to resolve clear cut cases of cybersquatting, it was not intended to resolve every trademark related domain name dispute.

However, ICANN's governance model can be a double edge sword. Specifically, the Registry and Registrar Agreements that provided the contractual means to enforce the UDRP on registrants also impose other contractual requirements on Registries and Registrars. Included in these contractual requirements is the need to collect, store and make available certain personally identifying information from registrants. This places registration authorities in the difficult position that in complying with its ICANN contractual obligations, it may be breaching national data privacy laws. While ICANN has implemented a process whereby registration authorities can seek a waiver, the process has its limitations. In fact, many in the ICANN community question whether ICANN's existing process will be able to scale to handle the new European General Data Protection Regulation (GDPR).

While relying on private communities may be a proven approach for addressing standardization and interoperability, private communities alone may not be capable of fully addressing “due process” and other legal and political issues that will arise with the use of digital identities on a cross-border, global basis.

9. A Public-Private Governance Framework

Instead of a purely private industry approach, we believe that the legal and political challenges in governance of digital identities will be better addressed through an appropriate public-private framework. Under this framework, private organizations would still drive consensus on standards and protocols relevant to blockchain solutions. But a public community—independent of any one sovereign state—would be responsible for obtaining consensus on the base governing policies and for moderating due process mechanisms. The (inter)operation of blockchain solutions by the private sector would remain free to evolve in an open and decentralized manner—bounded only by requirements promulgated by an independent public governance community specifically to address the conflicts of law, due process, and related issues with digital identity systems engaged in cross-border transactions.

We believe that an intergovernmental agency (or multiple IGO's in concert), working with affiliated government agencies in the various sovereign states is ideally suited for this public governance role, and early IGO involvement may help alleviate some of the challenges faced in the evolution of Internet governance.

IGO's typically provide an advisory, mediating, and liaison role already within the subject of their charter. Thus, they are well-versed in cross-border and global policy governance, and are

³⁹ <https://www.icann.org/resources/pages/help/dndr/udrp-en>

already positioned to work with sovereign governments in promulgating consensus policies, regulations, and due process procedures—both internationally and at a local level—for global digital identity.

IGO's and their affiliated government agencies are also uniquely qualified to help ensure parties transacting with digital identities could retain their ability to obtain legal redress within appropriate courts and administrative tribunals; and that policies and procedures appropriately balance differing views among sovereign governments as to data security and privacy rights.

The following chart is an example illustrating a public-private framework:

Governance Level	Governance Mechanisms	Governing Parties	Governance Model
International policy, regulation, and coordination	Consensus policies, applicable treaties, international law and tribunals	IGO (working with agencies of national governments)	Public
In-jurisdiction regulation and dispute resolution	Local law, regulations, courts and tribunals	National agencies (working with the IGO)	Public
Interoperation among blockchains, enabling technologies, IDP's, and service providers	Standards, protocols, open-source licenses, private contract (adhering to base requirements of the consensus policies)	ISO and participating standards bodies, industry organizations and working groups (working with the IGO and national agencies)	Private
Operation of individual blockchains	Private contract	Private companies and organizations (including national agencies as applicable)	Private

Two areas discussed previously underscore the need for independent public governance: ensuring the integrity of digital identities, and ensuring compliance with agreed-upon due process and conflict of law requirements to address disputes (whether between private parties or a state-based action).

If individual digital identity blockchain goes offline (either shutdown or interrupted) or is otherwise compromised, technical standards and compliance mechanisms must properly address maintaining the integrity of identities on that blockchain, transitioning them to another blockchain, or their removal as a valid identity. And, in the event of a dispute, these standards and compliance mechanisms must also properly enable access to information contained in, and associated with those digital identities to satisfy agreed-upon due process and other conflict of law requirements.

While private communities can efficiently drive consensus for these standards, there must be a governance authority that is sufficiently empowered to help ensure operators can be made to comply under applicable law in sovereign jurisdictions; and, conversely, to help ensure that an operator cannot be forced by any individual sovereign state to act contrary to those procedures.

10. Next Steps

InfoNetworks is currently evaluating a variety of blockchain related technologies. We are developing several projects to test solutions for the interoperation of digital identity blockchains that can be used for cross-border transactions. As part of these testbeds, we are also

researching and working with private and public sector partners on appropriate due process mechanisms for global digital identity solutions under a public-private governance framework as outlined in this paper.

We are also soliciting individuals and organizations from industry, government, and academia to engage with us in helping to establish the right governance model to foster better digital identity solutions while also addressing the legal and political complexities of data security and privacy rights on a global basis.

For additional information about InfoNetworks, please us at <http://infonetworks.global>, or contact the authors directly at: fcona@infonetworks.global or mpalage@infonetworks.global.