MIT Computational Law Report

Trust in a Trustless System: Decentralized, Digital Identity, Customer Protection, and Global Financial Security

Jonathan Askin, Chynna Foucek, Sydney Abualy, Alexei Furs

Published on: Jan 10, 2022

ABSTRACT

Propelled by globalization, technology, and geopolitics, financial crime represents a growing threat to the global economy while enabling terrorism, sexual exploitation, slavery, arms and drug trafficking, and wildlife poaching. To combat this activity, government regulators have passed a series of know your customer (KYC) and anti-money laundering (AML) measures requiring financial institutions (FIs) to conduct more thorough due diligence on customers and report suspicious transactions. Despite significantly increasing compliance budgets and investment, FIs have struggled to keep pace with these more stringent requirements. Rather than adopt new technologies to address the increasing volume and complexity, many companies are doubling down on legacy tools and expanding headcount. This paper examines the emerging concept of decentralized identity as a solution that can break this cycle and reduce financial crime by reviewing the technical components, regulatory environment, and pathways to adoption. In doing so, we hope to demonstrate how this transformative approach to conducting customer due diligence and reporting could enable FIs to reduce and mutualize the costs associated with KYC and AML while protecting the privacy of their customers.

Introduction/Description

Over the past 20 years, FIs have been challenged by a rapid intensification of KYC and AML regulation. Despite spending upwards of USD $500 million annually,[1] many FIs struggle to meet compliance requirements. In 2019 alone, 12 of the top 50 banks were fined for KYC and AML related violations, with individual fines eclipsing USD $5 billion.[2] Unfortunately, these fines and efforts have failed to significantly reduce financial crimes, with estimates of illicit financial activity climbing rapidly above USD $3.5 trillion per year.

At the same time, consumers are increasingly sensitive to the way their personal data is collected, stored, and retained. High-profile cyberattacks, like the 2017 incident against Equifax that exposed the sensitive information of more than 150 million Americans, have clearly demonstrated the pitfalls of mass collection of personal information. A recent report from Pew Research found 81% of Americans believe the risks associated with businesses collecting personal information outweigh the benefits.[3] In response, a number of new data privacy regulations, such as the General Data Protection Regulation (GDPR), the Personal Information Protection and Electronic Documents Act (PIPEDA), and the California Consumer Privacy Act (CCPA)

were enacted. These laws seek to limit the amount of personal data that businesses may collect, to ensure adequate protection, and to give users more control over their personal data.[4] Analysts believe there is a high likelihood of additional regulation in the years ahead, making it prudent for FIs to take proactive measures to incorporate privacy into the design of their applications.

Against this landscape, it is clear a new approach is needed to provide individuals with greater control over their data while making it more efficient for FIs to collect and verify the information necessary to satisfy KYC requirements. Decentralized identity focuses on providing a digitally native solution that prioritizes individual privacy while creating efficient methods for participants to share and verify information. By making it easier and more secure for users to provide information while also simplifying the processes companies under to verify the original source of the information, such systems can dramatically improve the efficiency of customer onboarding and compliance for FIs. In this paper, we explore the key mechanisms of decentralized identity, as well as its application to KYC and AML.

ESTABLISHING DIGITAL IDENTITY

Digital identity is a key enabler for digital commerce transactions and enables trust online.[5] The ability to identify and describe the real-world actor in the digital ecosystem is crucial to establishing trust, and providing the services we all enjoy including healthcare, education, and politics. Until recently, the process of identifying customers consistently forced FIs and other businesses to use time-consuming physical channels, including in-person meetings and wet signatures, to verify identity. Further, the information used to prove identity is established using onerous forms or paper-based documents that must be manually verified. Decentralized identity disrupts this process by enabling institutions to connect with and authenticate customers using purely digital channels. By encouraging common standards that allow information to be both verifiable and interoperable, this approach minimizes the need to independently verify and store redundant copies of information. While there are multiple approaches to implementing decentralized identity, the solution described in this paper is based on the Hyperledger Indy and Aries frameworks responsible for supporting different dimensions of digital identity.

Components of Decentralized Identity Solution

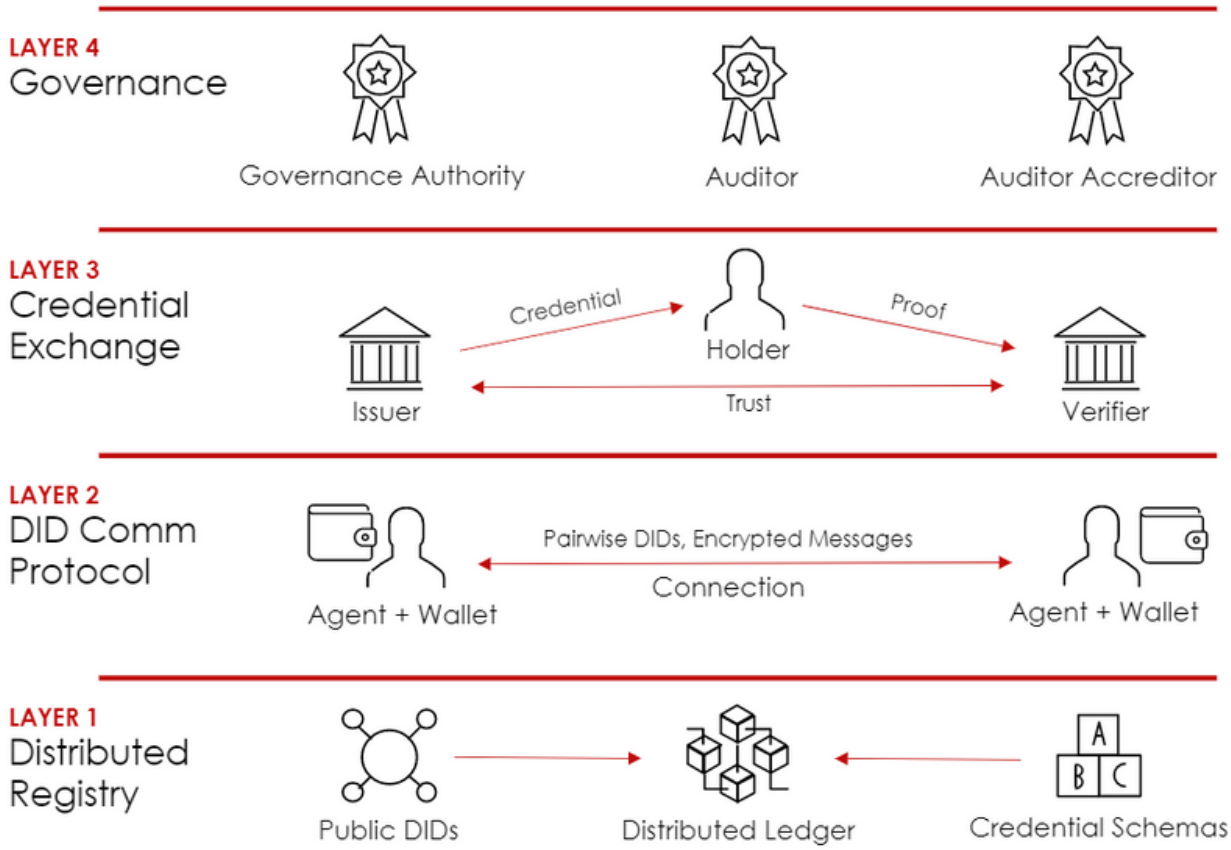

Figure 1. A conceptual architecture on how decentralized identity could be administered.

DISTRIBUTED REGISTRY

At a high level, decentralized identity uses a distributed ledger to provide a robust public key infrastructure and allow users to prove their identity using digital signatures without a centralized authority, as evidenced in the graphic in Figure 1. Distributed ledger technology (DLT) uses modern cryptographic techniques and a distributed ledger to provide a complete digital identity solution. As will be discussed in the coming sections, the solution can be separated into multiple levels, each redefined as a database that is distributed across multiple entities, that is only updated through a peer-to-peer consensus mechanism.[6] The peer-to-peer nature of distributed ledgers introduces the ability for information to be shared and trusted by multiple parties. Using such a ledger as a root of trust enables public keys and other data to be registered in a secure and immutable manner without a centralized party that could tamper with or censor data. Instead of storing identity information in a centralized database, individual users can hold digital credentials on their preferred devices.

These digital credentials can then be cryptographically verified using information registered on the ledger. In this way, the ledger serves as a critical foundation for the overall identity system. However, the security of the ledger is dependent upon the nodes that receive, validate, and record transactions. While similar to the nodes that support public blockchain networks, such as Bitcoin and Ethereum, identity networks are different in that they require some authorities to be known on the ledger so they can be trusted as the original source of information. For this reason, it makes sense to encourage a group of trusted bodies to administer the network, such as a consortium of FIs, whichstand to benefit from its use as a means by which to verify credentials presented by customers. Such participation would allow institutions to offer their customers improved experiences and more control over their personal data while simultaneously fostering interoperability between institutional stakeholders and therefore greater ability to share KYC information.[7]

IDENTIFICATION

Once the root of trust has been established using the distributed ledger, participants must establish a digital identity. This process begins with the creation of an identifier that is globally unique, resolvable with high availability, and cryptographically verifiable. Decentralized identity is based on the use of decentralized identifiers (DIDs), which can be generated, stored, and resolved without a centralized registration authority. The World Wide Web Consortium (W3C), the organization responsible for many crucial web standards including HyperText Markup Language (HTML), Simple Object Access Protocol (SOAP), and Extensible Markup Language (XML), has drafted a specification describing common standards for DIDs to achieve interoperability between identity systems.

For public entities, these DIDs can be published to the ledger[8] with the endorsement of a node operator, who would verify the real-world user matches the entity being registered. By using such decentralized identifiers, our solution enables participants to create identifiers for any type of entity, including people, businesses, and devices. The ledger acts as a source of truth by storing these DIDs in immutable transactions which can be queried and traced back to their source. Establishing such a ledger and allowing it to be publicly readable ensures a high degree of availability, transparency, and security. The DIDs stored on the ledger are intentionally public and therefore especially suited for identifying legal entities, such as governments and corporations.

There are also cases in which a user might not want to store a DID on an immutable ledger, such as when conducting personal business. For private relationships, DIDs can

be randomly generated and shared only between active participants. By using a unique DID for each relationship, users can interact with various parties without providing outside observers a means by which to correlate their activity. This is a significant departure from current identity systems, especially in the online ecosystem, where identity providers often track users by a single IDnumber or browser cookies. By supporting these pseudo-anonymous “pairwise” DIDs, as well as publicly resolvable DIDs published to the ledger, decentralized identity gives users the ability to choose their level of privacy. While pairwise DIDs can be used to receive and prove credentials, they should not be used to issue credentials, as the credential could not be traced to a public identity on a ledger by potential verifiers.

DIGITAL SIGNATURES AND AUTHENTICATION

Decentralized identity solutions rely on distributed ledger technology to verify a user's credentials and aspects of their identity. More specifically, a cryptographic signature acts as an identity’s securing seal. One widely used technique for authentication is to leverage cryptographic key pairs. These pairs include both a public key that is widely distributable, and a private key known only to the holder. By proving knowledge of the private key, a user can assert their identity. Knowledge of the private key is typically established by adding a cryptographic signature to a message. The message recipient can verify the signature using the public key of the signer. Because the signature is generated using the contents of the message in addition to the private key, the verifier can also know the contents of the message have not been changed, as doing so would invalidate the signature. Some of the most popular cryptosystems used to generate keys and signatures include Rivest–Shamir–Adleman (RSA) and elliptic-curve cryptography (ECC). Each system has trade-offs between speed, signature size, and security. RSA is an older, more established solution, but ECC can achieve an equal level of security with much shorter keys.

A key advantage of these new cryptographic signature systems is that the verifier only needs to know the public key of the signer to verify the signature. Unlike legacy government identifiers, such as Social Security numbers, there is no need for users to disclose their full key. This significantly reduces the threat of identity theft. Many jurisdictions, including the United States and European Union (EU), have recognized digital signatures as equivalent to handwritten signatures, and have codified their use as an acceptable means by which to authenticate users for electronic transactions. The E-SIGN Act, passed by the U.S. Congress in 2000, asserts that digital signatures cannot be denied legal effect solely because it is in electronic form. In the EU,

electronic identification and trust services (eIDAS) made electronic signatures valid as evidence in court, and defined multiple levels of signatures corresponding to increasing security requirements. At a minimum, the signatures used for decentralized identity would qualify as advanced signatures, which requires that the signatory be uniquely identified and linked to the signature, have sole control over the signature creation data (in this case the private key), and include a mechanism for ensuring the data to which the signature is attached cannot be tampered with without invalidating the signature.

If a cryptographic signature, the verification element of the digital identity solution, is legally recognized, it would greatly legitimize the framework in practice. The Blockchain Records and Transactions Act, introduced in the House in October 2020, seeks to amend the existing E-SIGN Act to clarify blockchain technology's applicability to electronic records, signatures, or smart contracts.[9] Under the act, records, signatures, or smart contracts cannot be denied legal effect, validity, or enforcement. Importantly, the legislation avoids constricting definitions of blockchain technology and smart contracts in order to allow for regulatory latitude in the future.[10] Further, the act would invoke pre-emption and prevent individual states from rejecting blockchain technology (specifically to ensure that states do not avoid granting legal recognition to blockchain records via reverse preemption).[11]

There are cyber risks associated with the shift to a decentralized system for AML and KYC verification purposes, including brute force, stolen keys, and distributed denial-of-service (DDoS) attacks to the ledger.[12] Additionally, there is the risk that poor-quality data might be entered into an identification wallet, which could lead to inaccurate data within the system that is distributed among various parties involved in the verification processes.[13] A decentralized model where one node is attacked could eventually compromise other notes within the chain, or specifically, those nodes that are most important.[14] However, compared to typical data storage techniques, a decentralized system is still more secure since identity providers no longer control a consumer's personal information.[15]

DESCRIBING IDENTITIES WITH VERIFIABLE CREDENTIALS

In addition to being able to uniquely identify and authenticate users, identity systems must enable attributes to be assigned to an identity to provide additional description. Such attributes might include everything from name and address to college degrees and credit score. In traditional, centralized systems, these attributes are typically collected from users by requiring the user to fill out forms. The data is then stored in a

database. As the user establishes additional relationships, they are often required to fill out forms containing the same information, and redundant copies of their data are stored in separate databases for each new relationship. As a result, personal data gets scattered across many siloed data stores, giving users little visibility or control over how their data is used. The high degree of friction introduced by requiring users to manually fill out forms makes it a challenge to keep data up-to-date and can act as a barrier for attracting new customers.

Decentralized identity addresses these issues by leveraging reusable digital credentials that a user can present to satisfy information requests across multiple relationships. These “verifiable” credentials include cryptographic signatures and other security measures that allow them to be traced to the issuer using the distributed ledger. These signatures also ensure the contents of the credential have not been altered, as changing the contents would invalidate the signature. The contents of the credential can be quite flexible and may include everything from simple text attributes to encoded media files. An example verifiable credential is shown below:

Example Verifiable Credential for Passport


```
{
  "witness": null,
  "signature_correctness_proof": {
    "se": "114253173041783977122360471664728364008160385216184096758557991239492875830595
```

```
  1562035942373605599877159435277724564849199437540789692103125119015440615707298957836117911
      "c": "735660300006756378351426824941728565285926875736661958665255153482748221975 41"
    },
    "signature": {
      "p_credential": {
        "m_2": "400586199074199186411895634140731804528933133779892666700526603481496999112 6
        "a": "122403463343657541761439063600239791236681993345546790615301425142590415707504
        "e": "259344723055062059907025491480697571938277889515152306249728583105665800713306
        "v": "100003126484989002179368789471447048072221691125325639554453937846828609173594
      },
      "r_credential": null
    },
    "values": {
      "street_address": {
        "raw": "123 Test Street, Council Bluffs, IA, USA",
        "encoded": "58036933892885198598151043457314034905094923607565735621681686536414789 5
      },
      "country": {
        "raw": "US",
        "encoded": "70165353610619518311701925933431423754671612649169184380883946982998843 4
      },
      "expires": {
        "raw": "1646179200000",
        "encoded": "41384461911882109336752680276721955494511849396983517814707275094827459 8
      },
      "id_no": {
        "raw": "100003106",
        "encoded": "100003106"
      },
      "birthdate": {
        "raw": "1109635200000",
        "encoded": "47978928771762490053781789644904548202419063866684834711585707040246722 0
      },
      "locality": {
        "raw": "Council Bluffs",
        "encoded": "84761748859675091076401984331563780505106818472993711577828529671952838 5
      },
      "id_type": {
        "raw": "Passport",
        "encoded": "22367854443955698103410235929499018869582959010445656057570366099425223 6
      },
      "government_id": {
        "raw": "123-45-6789",
        "encoded": "74432686711966281305857415171057226008648098777873599038544473559438578 1
      },
      "given_name": {
        "raw": "John",
        "encoded": "76355713903561865866741292988746191972523015098789458240077478826513114 7
      },
      "region": {
        "raw": "IA",
        "encoded": "75700607342123578529824411558309803434466834710069063661458099476185679 2
      },
      "postal_code": {
        "raw": "51503",
        "encoded": "51503"
      },
      "family_name": {
        "raw": "Doe",
        "encoded": "11458345205666507217595416908009131926495431666498934306091548306482523 8
      }
    },
    "schema_id": "EjLZmrFYeW7EWVCTJudkfC:2:Government eID:1.0.0",
    "cred_def_id": "EjLZmrFYeW7EWVCTJudkfC:3:CL:53:default"
  }
```

The process of issuing a credential starts with an authoritative source such as a government, a FI, or other trusted entity. Credential issuers can register standard schemas to the ledger that will define the properties and structure of credentials that will be issued. These schemas are crucial for enabling interoperability, as well as supporting more advanced behavior, such as zero-knowledge proofs, which will be discussed later in this paper. An example schema is shown below:


```
{
  "auditPath": [
    "6c4eR2Vzv3dWCYk7nj7cHKPE8ESDU9jkRNZ3x3P3GEBD",
    "9jSnd6VhjpnYa5YvSbdC5uKX6QP9s6pyyuqBEiLXvzVm",
    "2sXWzU5cgavK4jYTZYpmyp5eBJMsfLHCNGxreMwRAap9",
    "2G3SGzfHtxsVRUbx2jZeWE1RKM5bY8DFucgbgL9SpzrN",
    "DVHkg75xAf9WqXHNezuqrMh9B9JFbzWTQY8A9kq9B2uH"
  ],
  "ledgerSize": 56,
  "reqSignature": {
    "type": "ED25519",
    "values": [
      {
        "from": "EjLZmrFYeW7EWVCTJudkfC",
        "value": "je61ZF5CXCx99BiLsoL4okDGrwLzEYMN6rnhGn6DKdLrfHgLrbH8FAfy1P3p7F9bzSje6i23
```

```
1gCMaiUG3GKGSfM"
      }
    ]
  },
  "rootHash": "HLATqp3C6monrGQsu3rcDiaEgDP4uxsNWSNmzURCDZrB",
  "txn": {
    "data": {
      "data": {
        "attr_names": [
          "given_name",
          "street_address",
          "id_no",
          "expires",
          "family_name",
          "region",
          "id_type",
          "birthdate",
          "government_id",
          "postal_code",
          "locality",
          "country"
        ],
        "name": "Government eID",
        "version": "1.0.0"
      }
    },
    "metadata": {
      "digest": "0800d8435daf3f0cb2f59a097424c07861770c4ce97b09877403cf33ab86ae89",
      "from": "EjLZmrFYeW7EWVCTJudkfC",
      "payloadDigest": "9cf72046f4d7bab9fdbfecac39881761ca86c5f0fbbf5b6f9a7aac4d459e9d38",
      "reqId": 1612547370331770400
    },
    "protocolVersion": 2,
    "type": "101"
  },
  "txnMetadata": {
    "seqNo": 53,
    "txnId": "EjLZmrFYeW7EWVCTJudkfC:2:Government eID:1.0.0",
    "txnTime": 1612547372
  },
  "ver": "1"
}
```


Once a schema has been registered, multiple issuers can register on the ledger to issue credentials using that schema using a mechanism called a credential definition, which includes a reference both to the intended schema, the issuing identity, and the public component of the keys that will be used to sign the credential. An example credential definition is shown below:


```
{
  "auditPath": [
    "8JvSnRjixrxr6bG1jLhVSy8WNMbnTuNvHNjhbpjNgbzG",
    "9jSnd6VhjpnYa5YvSbdC5uKX6QP9s6pyyuqBEiLXvzVm",
    "2sXWzU5cgavK4jYTZYpmyp5eBJMsfLHCNGxreMwRAap9",
    "2G3SGzfHtxsVRUbx2jZeWE1RKM5bY8DFucgbgL9SpzrN",
    "DVHkg75xAf9WqXHNezuqrMh9B9JFbzWTQY8A9kq9B2uH"
  ],
  "ledgerSize": 56,
```

```
  "type": "ED25519",
      "values": [
        {
          "from": "EjLZmrFYeW7EWVCTJudkfC",
          "value": "2Q3viZVGnLAQfsZYXDy59nqfowpJKskYaob3dwyp19xqrt4ZxsuLGjndH9vns2oshCDvk1uZ
        }
      ]
    },
    "rootHash": "HLATqp3C6monrGQsu3rcDiaEgDP4uxsNWSNmzURCDZrB",
    "txn": {
      "data": {
        "data": {
          "primary": {
            "n": "123206747739403544701653647329843865912950405707141818684827350404724575538
            "r": {
              "birthdate": "105601766913585705409434042851055451198601909775127736847420885
              "country": "134658294302919124692513354594081797992008769482697051841996899560
              "expires": "705214133522479607856826491479910113529496609379816787185985788284
              "family_name": "117404876424026103565419682977691920358899438009558531388061396
              "given_name": "529120275657544877231512531508237190433489595374408471075122878
              "government_id": "229269415768399367311617624786692694029034520468602053360467
              "id_no": "153133424838900381411006746646534305735410895630065289028386728347933
              "id_type": "601562348039289834799752029618824957905965143223472924533527711593
              "locality": "110584783685812131088013062602761770501816291098380413441946566222
              "master_secret": "526976578071110141026085376082255739522064535392224380578084
              "postal_code": "767397436895006827647582369919764456421834806589341371801103499
              "region": "348536532854280129764014070328732510288905900601195359001558850246222
              "street_address": "391219176779114817935035370084652862299011543085995905094899
            },
            "rctxt": "118210195449177261758568240285293465971024130992815532346280214113289595
            "s": "859542094870761389246566985570915012734126448836812481789133285309962915855
            "z": "371313357433758821842650260301615075132617079141502770894347247979915573995
          }
        },
        "ref": 53,
        "signature_type": "CL",
        "tag": "default"
      },
      "metadata": {
        "digest": "25f5366ecb67efb5dad488d5cdf3fcb7229d90238dc246760f36fd1ab1f1a008",
        "from": "EjLZmrFYeW7EWVCTJudkfC",
        "payloadDigest": "70a071845bd1057be6ed7e86e0199518ca7192b41ea0e7be5b899f38e2b6b817",
        "reqId": 1612547386817756000
      },
      "protocolVersion": 2,
      "type": "102"
    },
    "txnMetadata": {
      "seqNo": 54,
      "txnId": "EjLZmrFYeW7EWVCTJudkfC:3:CL:53:default",
      "txnTime": 1612547388
    },
    "ver": "1"
  }
```


At this point, the issuer is ready to issue credentials. In order to create the credential, the issuer can collect information from the user via a webform or other means or use information collected independently. The issuer sends the credential to the user's identity wallet using an encrypted channel.

Just as important as the contents of the credential is the identity of the issuer. As previously discussed, the issuer must be registered on the ledger. While a user is free to share credentials with other parties, the verifiers may only choose to trust credentials from reputable sources. Here lies the opportunity for FIs and other trusted entities to take on the role of authoritative sources to issue credentials.

Policy and Regulations Surrounding Online Verification of Identity

As a potential issuer of digital credentials, government agencies play a crucial role in digital identity authentication. As such, it is imperative that regulators and legislators recognize the value that trustworthy digital identity solutions offer, introduce policy for widespread adoption, and encourage collaboration among public and private sectors. Currently, the United States stands well behind the other nations, primarily the EU, in implementing a regulatory framework for secure digital identity authentication. Given legislators growing concern with financial crime, 2021 is likely to bring innovative policy measures to protect consumers' privacy.

The Improving Digital Identity Act of 2020 is recent bipartisan legislation introduced in the House in September 2020 to address the threats that organizations, businesses, and government agencies face when it is unable to reliably verify an individual's identity in online transactions.[16] The act points to impending cyberfraud and crime as motivation to implement trusted digital identity solutions, however, notably, the legislators recognize that an innovative digital identity solution would allow for greater access to digital financial services and promote financial inclusion.[17]

The act calls for (1) a task force to establish a government-wide effort to develop methods for federal, state, and local governments to validate “identity attributes,” and implement an interoperable solution to encourage mass adoption across states; (2) the National Institute of Standards and Technology (NIST) to create a framework of standards for government agencies that provide digital identity verification services - with an emphasis on security and privacy, and; (3) a grant program within the Department of Homeland Security for states to upgrade their methods of issuing identity credentials and further support an interoperable state framework to enable digital identity verification in accordance with NIST’s standards.[18] The act suggests that state governments are particularly well positioned to “play a role in enhancing digital identity solutions used by both the public and private sectors,” - specifically, as authoritative issuers of identity - as state governments commonly issue identity documents, such as drivers licenses.[19] Further, the legislators note the importance of

public and private sector collaboration, as "[t]he private sector drives much of the innovation around digital identity," especially in delivering digital identity solutions.[20]

Legal liability surrounding a DLT system is uncertain, due to the novelty of the technology and because many national and federal governments do not yet have blockchain law or doctrine built out yet (if at all).[21] In the financial sector, there is often a central party that is heavily regulated and held accountable in the event something goes awry in a specific financial transaction or process.[22] "However, in many blockchain use cases there is no such centralized party that takes responsibility for the provision of services or controls associated data sets."[23] While existing law can be applied in the context of DLT to the KYC and AML processes, there is uncertainty as to how those laws will specifically be applied. FIs should rely on counsel to "look at the legal system as a whole and apply the system's foundational principles"[24] through the lens of traditional legal practice areas, such ascontracts, torts, and property.[25] Additionally, because a decentralized ledger provides the opportunities for other FIs and customers to participate from across the world, questions remain as to which jurisdictions' laws would apply in the event the KYC or AML verification process caused issues.[26] Because KYC and AML verification using DLT will operate as a private system, FIs can develop internal frameworks and contracts that will lay out what law and jurisdictions shall apply.[27]

COMMUNICATING AND SHARING CREDENTIALS

Once a digital identity is created and associated with an individual or entity, that digital identity can be used to conduct transactions and otherwise assert identity just like a traditional form of identification. When a user attempts to access a system, the system will assume the role of a verifier that collects and verifies credentials from the user. First, the verifier will form a connection to the user. This is typically done by presenting the user with a QR code that will establish communication between the parties and allow the user the ability to create a new pairwise DID for this relationship.[28] Once a connection is established, the verifier will send a proof request, which defines the requirements that must be satisfied to verify the user's identity.[29] This may include asking for a particular type of credential, such as a digital driver's license, as well as the specific properties of the credential that must be provided. The user then consents to provide the information required and presents their previously issued credential to the system in the form of a cryptographic proof that satisfies the request. This proof includes digital signatures and additional measures that prove the user is the valid holder of the credential and that it has not been tampered with.

Finally, the verifier cross-references the signatures within the proof and verifies that it matches the key registered on the ledger by the issuer of the credential.

The presentation of a credential takes the form of a zero-nowledge proof that can obscure any personal information when it is not relevant to satisfying the proof request. A zero-knowledge proof is a method by which one party can prove to another a certain fact, but not reveal the underlying data to make that assertion. For example, such a proof could allow a party to prove the date of birth within a credential is after a certain date without needing to provide the actual date of birth. These protocols are combined with blockchain technology to create a system where, depending on the requirements of the transaction being conducted, minimal information about the entity conducting the transaction is stored in the transactional system. Only the original certification authority has the complete information about the owner of the credential; any transactions then conducted with that credential do not require further presentation of personal data by the credential holder.

By creating a system that allows for the reuse of credentials, there is a massive reduction in identity verification time and costs. A reusable credential for KYC purposes would be where one bank and/or central authority conducts the KYC process one time on an individual and then shares the results in the form of an issued credential to the entity requesting verification. Now, the owner of that credential is free to conduct business with any organization that respects the KYC process of the original certification authority. The result of a system like this is the mutualization, or sharing, of costs to conduct KYC only once per individual across the whole system of participating organizations. Because the credential being issued conforms to standards set forth and agreed to by the group, there can be no doubt the credential will have the proper amount of data and verification completed before the credential would be provided. An interesting question arises about the governance and self-policing needed by a system like this. If a certain organization that is granted the ability to provide identity credentials and/or KYC credentials is consistently not meeting standards set by the overall group, then they must be evaluated and removed. Luckily, due to the immutability of a distributed ledger, it would be quite simple to re-evaluate the credentials that organization had provided by simply looking up transactions with their public key as the KYC provider.

APPLYING DECENTRALIZED IDENTITY TO KYC AND AML

The basic purpose of KYC processes is to create a complete and accurate identity profile of the customer. In addition to asking the customer to provide information

about themselves, FIs also leverage data from publicly available sources, as well as purchasing data from third-party services. The type and amount of data collected depends on the client. For individual clients, this includes personal information, such as legal name and address, and other information, such as sources of income and political exposure. Corporate clients may require tax identification numbers, articles of incorporation, and ultimate beneficial ownership to be collected.

Current Methods of KYC

Currently, compiling such information can be an expensive and labor-intensive proposition, pushing many FIs to leverage proprietary vendors to augment their own records. The current vendor landscape includes companies that specialize in providing sanctions and watchlist data, negative news and politically exposed persons (PEP) data, information on individuals, such as biometrics and online behavior, corporate structures, relationships to other entities, geographic data, and a whole slew of tools to integrate, clean, and visualize this data into a comprehensive picture of an individual identity.[30] FIs can stitch these services together on their end in conjunction with their proprietary data or rely on the vendor for wholesale creation of an entire data set. However, despite the advantages to the KYC process, the creation of these large datasets creates significant data privacy concerns for the individuals. Based upon the extensive network of players, this has led to a number of issues, such as potential exposure to data breaches, as well as lack of standardization of data sets.

Relying on a large network of vendors to provide data into the KYC process has led to a system that has many points of entry for nefarious actors. By making this data into a financial honeypot that can be sold and traded, for both legitimate and illegitimate purposes, any vendor or FI hosting large collections of KYC data becomes a target. This has been evidenced many times over recent years, but one of the most newsworthy was the 2017 hack of the credit bureau Equifax.[31] Through an exploit of an out-of-date web framework on a credit dispute website, hackers were able to enter Equifax systems, gain credentials to other services, and ultimately walk away with Personal Identifiable Information for more than150 million customers. In this hack, the 150 million victims had no say in how their data was stored by Equifax, and likely did not know their data was even permanently stored by Equifax. Similar hacks coupled with the demand for cryptocurrency ransoms (ransomware) have taken this attack vector to the extreme since 2017, exploiting the huge negative press that was attributed to Equifax to pressure other vendors and FIs into paying massive sums to avoid exposure.

Furthermore, relying on multiple vendors to handle KYC data processing and storage has led to a system of competing data standards. Any vendor who participates in this ecosystem can develop their own schema to store their data, and likely would use this as a differentiator in marketing their proprietary datasets to FIs, marketing their schemas as built for speed, including additional metrics for risk analysis, etc. This lack of an overall industry-standard data schema makes the integration of data across multiple sources difficult. This results in the need for data cleansing and translation by FIs in order to integrate all their data sources into one system, creating even further redundancies in data storage of sensitive information.

Recently, the Financial Crimes Enforcement Network ("FinCEN") at the U.S. Department of the Treasury proposed new requirements specific to virtual currency transactions, "*Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*."[32] FinCEN's motivation for this proposed rule is to mitigate illicit financial transactions, such as fraud and money laundering, seen in virtual currency transactions held by "unhosted" wallets and wallets hosted in foreign jurisdictions without sufficient AML protections. The requirements would place new recordkeeping, reporting, identity verification, and collection requirements on banks and money service businesses (MSBs) that employ certain transactions involving convertible virtual currency (CVC) and digital assets with legal tender status (LTDs).[33] This proposed rulemaking was received by the industry with criticism and controversy; notably, it would require banks and MSBs to manually collect and report information, such as the name and physical address of unhosted wallet counterparties for CVC/LTDA transactions that exceed a certain monetary threshold. This requirement is antithetical to the pseudonymous nature of digital asset transactions, as well as places overly burdensome reporting requirements on the affected firms. As of January 2021, FinCEN is still reviewing industry commentary before it enacts its final rulemaking, however, the proposed rule speaks to this regulatory perspective requiring bolstered KYC and AML procedures to support not just digital assets, but more generally, an innovative financial ecosystem.

DLT Policy: Moving Forward and Legal Implications

The decentralized ledger technology platform, with the potential to stand as a more secure and efficient option to identify verification, creates questions as to who is liable for the verification process in the event the KYC or AML data ends up being incorrect.[34] Both with and without the DLT platform, a FI must undertake due diligence to reject or validate a customer. However, in a decentralized system, once this validation has

occurred, “it stores a digitally signed document in the smart contract of this customer and this includes the result of the core KYC verification process (verified or rejected),” in addition to the documents submitted by a customer.[35] Financially, it appears that a DLT platform would reduce the costs of conducting KYC and AML verification processes and ultimately, spreading out financial risk among all FIs who choose to work with a specific customer.[36] Once a customer has gone through an initial verification process, he or she can choose to share the private key with other institutions. However, for additional FIs to access the ledger, and utilize the information garnered from the core KYC and AML processes, some have proposed models that require FIs to pay the proportional part of the average price of conducting a core KYC verification process. Through smart contract adding, it can be guaranteed that “all the FIs that work with one given customer share the costs of the core KYC verification process proportionally.”[37]

To date, there seems to be no consensus as to who would ultimately incur legal liability in the event that information was incorrect or KYC or AML verification processes were still violated. Presumably, it could be argued that the core verifying FI bears the same responsibility as it would under existing processes. However, as mentioned earlier, each FI still bears the responsibility to conduct adequate due diligence and thus all participatory banks would probably be liable and subject to KYC or AML noncompliance fines. Additional FIs should not remain passive once the core verification processes have been conducted and should analyze the ledger to see how many institutions have worked with the customer so far and review customer credentials themselves. However, a DLT system may provide a clearer pathway for regulators “to easily and routinely check the KYC process,” through following the clear record laid out within the system.[38] Importantly, the ledger could “serve as a single point of truth” when there are disputes and issues.[39]

Concerns over privacy and the degree of trust that is afforded to DLT are two major points of apprehension that continue to inhibit widespread adoption within the financial space. Foundational questions like where financial information is securely stored, whether on the DLT itself, or on external data repositories with only credentials stored on the DLT, must be agreed upon by both stakeholders and policy makers. Issues around data security still need to be addressed as privacy will still be a serious concern. New attack surfaces will emerge that differ from that of centralized databases. Finally, the degree of trust afforded to DLT as a verifiable source of truth also poses risks, as like any database, DLT suffers from similar issues with respect to the credibility of data. DLTs immutable attributes on one hand may guarantee

consistent information, but additional safeguards are required to ensure the verifiability of information as it is entered onto the DLT.[40]

While a decentralized approach to KYC and AML enables FIs to meet the requirements of KYC and AML verification through the establishment of a digital identity, there are risks associated with the retention and processing of information used in verification among the technology's various nodes. Notable is the potential for the disclosure of sensitive financial information, since sensitive and personal identifying information is necessary to meet KYC and AML requirements. In Europe, for example, there are concerns that verification on the ledger could signal to others that a major transaction is to occur, leading to insider trading and price manipulation.[41] Further, a lack of regulation in the realm of transactions that occur on the blockchain could exacerbate the chances that insider trading occurs.[42] FIs should be quick to monitor for instances of insider trading and, in addition to bringing civil charges, should ensure that authorities properly prosecute those who misuse the decentralized system for their own gain.

Alternatively, a self-sovereign model, in which corporate customers create and manage their own identities, can put the onus back on the user, minimize liability on the part of the banks, and ensure identification is accurate. In creating and managing their own identities, users will compile the relevant documentation on a decentralized platform and grant permission to multiple entities/banks to access that data. Via a decentralized platform, each entity would be able to communicate and share relevant verification information with each and every user on the network via a private peer-to-peer basis. A self-sovereign model will not only allow for customers and users to take control over their identities but allow FIs to focus on verification and authentication rather than having to create and store identities themselves. Additionally, some of the privacy implications are mitigated, since the identity is not stored with the FI indefinitely, but represented by the key and linked to a distributed ledger.[43] This reduces some concerns regarding security vulnerabilities related to the information the bank holds on to.[44] A decentralized model also allows multiple FIs to leverage the same credentials and, ultimately, lessens the burden of KYC and AML requirements by no longer requiring each institution to repeat the verification process over and over again.

The proof mechanism of decentralized identity creates new opportunities for banks to safely accept credentials from customers that were issued from authoritative sources and mutualize the costs associated with KYC in a way that still enables data privacy protections. However, different models exist that could alter the legal implications and

legal responsibilities of banks that request information for customers and confirm the credentials.[45] Under a bank sharing model, one of two methods of collection among banks could occur.[46] For example, data collection for verification could include both customer-provided facts and also redundancies between banks that aren't customer provided.[47] However, this might introduce legal issues and concerns related to customer data privacy, especially for individuals who fall under GDPR legislation or state-based legislation like the NYDFS.[48] Additionally, a model could be set up that allows banks to collaborate in not only the sharing of customer information, but in the performance of due diligence of customer information, as well.[49]

While this decentralized approach does improve data collection and make the verification process more efficient, ultimately each bank would still need to provide some form of their own due diligence; primarily, the forming of an opinion as to whether the customer passes the KYC and AML checks once they have received the data through the decentralized platform.[50] Due diligence (and liability) for their customers would still remain with each bank, and banks would still be subject to fines for non-compliance on the part of customers performing illegal activities.[51]

However, FIs can place most of the onus back on the user by laying out the terms of arrangement in a contract before allowing for a customer transaction.[52] These contracts should detail the relationship between the FI and the customer, with the rights and responsibilities of each laid out.[53] Because the bank will have less control over customers' data, the contract can grant permission on the part of the customer to release data to the FI.[54] The agreement can also lay out ramifications and liabilities if the decentralized system is used maliciously or illegally and provides FIs with incorrect information. If a customer has multiple receivers of their information, then a legal agreement can exist with each entity, however the same data and mechanism to provide the information to the various banks is utilized.

Moving toward a critical mass

Education and incentivization for users to take part in a decentralized Know Your Customer platform is necessary foradoption of the system and movement toward a critical mass of users – both as FIs and as customers. Part of the difficulties that existing centralized corporate KYC utilities currently face is that there are competing solutions, which means customer data is segmented and siloed across separate databases. Thus, industry standardization via a single solution, as well as interoperability among FIs are crucial to achieve the movement to a critical mass of users.[55] The variety of identity service providers and client data utilities has led to

competing identity schemas and identifiers. For a decentralized corporate KYC approach to be most effective, the financial services industry should look at adopting a common set of standards and data schemas to avoid complications from cross-platform data transfer and allow for easier movement of data and information.

Role of the Government in Encouraging Digital ID Adoption

From a policy perspective, government entities can and have played a crucial role in fostering the establishment and mass adoption of its citizens digital identities, especially in countries outside of the United States. In the wake of the covid-19 pandemic, the need for digital identity to give users control over their credentials and establish harmony between the public and private sector and is tantamount to rebuilding the economy and fostering trust in the government at the national and global level.[56] The Republic of India's Aadhaar Act of 2016, for example, called for the design, development, and deployment of a national digital biometric identity system, to account for over one billion people in the country and in the database.[57] Through the establishment of digital identities, the Act aimed to verify identities for government processes and services, such as obtaining a driver's license or government benefits, as well as for authentication by private companies.[58] Additionally, in 2016, the Digital ID & Authentication Council of Canada issued the Pan-Canadian Trust Framework overview, which sought to bolster Canada's participation in the global economy via the creation of digital identities and digital transactions.[59] The framework aims to encourage public-private collaboration to adopt and implement digital identity services while overcoming the challenges associated with a digital identity system.[60] In September 2020, the Council launched the actual framework, that included "a set of digital ID and authentication industry standards that will define how digital ID will roll out across Canada."[61] The coronavirus pandemic bolstered efforts to adopt a national digital identification system, as the county has begun initial operations and alpha testing in the hopes of launching a national system within the year.[62] Finally, the European Union's Electronic Identification (eID) and Trust Services are a third example of government promulgation of a national digital ID system. Under eIDAS regulations, promulgated in 2014, people and businesses were able to use their country's eIDs to access public services online in European Union countries and created a European market for these services. By allowing for cross-border interoperability for services like electronic signatures and time stamps, the European Union aimed to incentive use of the digital ID to conduct operations.[63] This led to vast digital growth while promoting transparency within the framework.[64]

Something to consider is the legality of sharing a national ID system with the private sector. In 2018, for example, the India Supreme Court ruled that private companies' use of Aadhaar identification was unconstitutional.[65] Section 57 of the law permitted the state as well as any corporate body or person to use Aadhaar "for establishing the identity of an individual for any purpose".[66] Critics of the ruling noted that the court excluded all private sector entities but not public sector corporate bodies, creating inconsistencies in the ruling in relation to the statutory language.[67] However, in response to this ruling, India's legislature amended the Aadhaar Act to allow for private entity use upon voluntary permission by the customer.[68]

While governments should highly encourage the use of digital identities for both government services and private economic transactions, it is important to note that based on a country's laws and founding documents, mandatory use may be illegal or unconstitutional. Thus, countries should focus on a voluntary national digital ID system that encourages users to participate in the system, and further, provides all residents with the technology and educational tools to understand and use the technology. It is also important to note that national digital ID programs should be supplemented with strong national privacy and security laws and strict ramifications and protections in the event that there is a privacy violation. "Building trust with citizens around the secure usage of personal data will be key to creating effective frameworks."[69] The European Union is a prime example of a government body that leverages a strong set of privacy laws to bolster its digital identification program. In contrast, India lacks strong data privacy laws, and while offering some protections in the Aadhaar Act and penalties for misuse, may pose a detriment to widespread adoption if privacy is not adequately protected.[70]

Managing Client Risk by Ensuring App Security

FIs should also work to encourage customer use of the identity wallets and the setup of verification keys by ensuring application security and minimizing the threat of financial and legal risk when using an application. By implementing privacy-by-design elements during the creation of a digital wallet, consumer concerns about privacy and security are mitigated. For example, encryption methods and mobile software security solutions can provide added protection to decrease cyber threats. Notably, blockchain solutions, such as Identity Management, generate more secure applications by giving consumers control of their credentials.[71] This minimizes handling of sensitive personal identifying information on third party databases or servers. Consumers should have agency in deciding which information is shared and companies should consider what is necessary to verify identities. A solution could also include verification processes that

vary in terms of requiring a certain level of specificity for credentials. FIs should seek to obtain as little information as needed for the verification process to protect privacy and minimize the amount of potentially exposable information, especially because any data added to the blockchain is permanent.[72]

However, there are some risks associated with using an application like a digital wallet, including private data leaks, metadata tracing, replay attacks and impersonation, and a private key compromise.[73] Additionally, "as more and more individual metadata is shared with various relying parties and credential issuers, it can be correlated with onchain data in order to link users and their activities."[74]

To manage security risks, FIs can look to trade groups, such as NIST, for guidance. NIST plays a critical role in the marriage of private sector and government cybersecurity practices through its publications, which detail best practices and recommendations for the technology sector.[75] The standards developed by NIST are derived from conversations among industry organizations and documents, like security documents and publications.[76] NIST guidelines are valuable and have been used in the public and private sectors to evaluate and appropriately deal with cyber risk.[77] NIST recommendations are not binding, but they can encourage the private sector to adopt appropriate security measures that minimize the threat of attack through strict requirements and public-private sector collaboration.[78] Failing to implement appropriate cybersecurity features can lose a company business, damage its reputation, and affect performance levels within the institution.[79] While NIST compliance can provide an added layer of assurance that a company has implemented industry best practices,[80] it can also provide peace of mind to customers and government agencies by reassuring them that even in the event of a cyberattack, a company has done the best it can to secure its infrastructure and protect data. In 2020, NIST published a whitepaper titled "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems," which categorized various blockchain management systems into a taxonomy "based on differences in blockchain architectures, governance models, and other… features."[81] The paper goes into detail about emerging standards and details security and privacy considerations crucial to the development of a secure identity management system.[82] Importantly, FIs should "carefully monitor the validators' activity and establish security thresholds and metrics to ensure that the increased risk of attacks on a declining blockchain are understood and considered acceptable."[83]

Fostering Trustworthiness to Encourage Adoption and Use of Identity Wallets

The adoption of identity wallets by users is hindered by the technical complexities that result from the existence of multiple applications and the movement toward a critical mass. However, even with multiple applications on the market, there are some cross-ledger solutions that could help move toward a critical mass by allowing for integration and/or consolidation into a larger structure. For example, incorporating a universal resolver system into the blockchain can achieve compatibility among different identity management systems and ultimately the creation of a common user interface. Additionally, "the capabilities of a given system may be integrated into another system by implementing the libraries provided by the former system in the form of onchain logic in the latter system."[84] Tools like smart contracts exist that can integrate certain ledger capabilities into platforms.[85]

To encourage users to adopt identity wallets in the self-sovereign model, it is crucial for FIs to foster trust frameworks, display and ensure the systems' are technically sound, and advocate for regulatory frameworks within the space.[86] "Trust frameworks consist of a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose."[87] FIs should create governance models that lay out the policies, standards and responsibilities for users of the decentralized system. Due to the unique features of self-sovereign identities, a trust framework is necessary to lay out how users should interact on the system in order to maintain proper use.[88] "For citizens to trust and be willing participants, organizations must take the time to contribute to the global dialogue between trust frameworks and explain their models clearly. Innovative thinking is needed to enable citizens of all backgrounds to participate in this digital public infrastructure."[89]

Solutions and Call To Action

To implement a successful KYC methodology that relies on decentralized identity, FIs must work together with the United States government to help establish national digital IDs that can be used for verification purposes and for financial transactions and are compatible with systems worldwide. FIs and other companies that utilize digital technologies should work to lobby the government to adopt a national digital ID system, emphasizing the importance of digital ID in giving an identity, and thus access to government and private sector programs to those who may lack the resources to obtain a traditional government ID like a passport or driver's license. Provided consensus for a digital ID is achieved at the federal level, a framework must be set up to account for the use of the decentralized identity technology both in and outside of

the United States. The government should use a framework to define and establish what public programs and private sector initiatives should be included.[90] FIs can garner support for the digital ID to function in the context of financial transactions by showing the positive effectdecentralized identity can have not only on the KYC and AML verification processes, but on the autonomy that is given to the consumer/customer via control of their credentials. Additionally, for a decentralized KYC system to truly reach general consensus and protect consumers, FIs must also advocate for the establishment of federal privacy and cybersecurity laws.[91] However, because of potential privacy concerns and the risk that some may not have the resources or skills to establish a digital identity, the federal government, and the private institutions it selects to include in the framework, should ensure the program remains optional and provides customers with an affirmative option to voluntarily participate.

“For citizens to trust and be willing participants, organizations must take the time to contribute to the global dialogue between trust frameworks and explain their models clearly.” Innovative thinking is needed to enable citizens of all backgrounds to participate in this digital public infrastructure.[92] FIs should strive for universal coverage in encouraging the adoption of digital IDs and use of the technology for KYC verification. The world economic forum has highlighted principles of universal coverage that should be prioritized when developing a digital identity system, such as non-discrimination and inclusivity, affordability, and accessibility.[93]

“Not having a digital identity should not exclude a person from receiving the basic services that the government is mandated to provide,”[94] and FIs should focus on equitable access to services. “Digital identity programmes administered or coordinated by public agencies must be created with the understanding that lack of internet access can exacerbate the exclusion of citizens, especially when their capacity to access government services, legal entitlements, or conduct transactions is linked to an identity ecosystem that requires constant connectivity for regular authentication.” FIs and other private sector companies can play a role in achieving an equitable decentralized system through equal access to technology initiatives and by educational programs and advertisements that educate and incentivize community members to partake in a digital identity system. These initiatives will help build relationships and trust among FIs and the community and inspire customers to use the proposed decentralized identity systems.

Finally, financial institutions should embrace strict oversight to foster transparency and build trust with users and the government.[95] While decentralized identity systems can play a role in ensuring regulatory agencies have access to verified and accurate KYC and AML information, thus incentivizing FIs to adhere to regulations for fear of fines, more can be done to ensure the proper regulatory framework exists at both the national and worldwide level. Because FI transactions can be international, a decentralized identity system can benefit from the establishment of a think tank or multinational organization to oversee and set the framework for use of the technology for KYC and AML purposes and properly enforce protocols. This should be a public-private partnership, comprised of regulatory experts who understand the regulations for KYC and AML processes, as well as trained privacy and blockchain professionals to set appropriate operating standards and requirements. An entity comprised of both technical and regulatory professionals at the multi-national level will ensure governments and financial institutions properly implement a digital identity system that protects users privacy while allowing for more efficient and accurate KYC and AML verification.

Conclusion

Account opening and KYC processes continue to be one of the biggest costs for FIs every year. In fact, account opening processes and technologies have been cited as the biggest priority and spend for the past three years by CIOs of leading FIs.[96] Despite the high spend on these systems and processes, FIs continue to pay high fines every year for failing to recognize or ignoring the risks of with whom they are doing business. In 2020, more than 12 billion euros of fines were handed out to banks globally, with 9 billion of that coming from the United States.[97] These fines run the gamut from AML to KYC violations, but the majority of them come down to doing business with an identity they should not have conducted business with, and/or not doing proper due diligence on the identity of an individual or entity. Combine these consistent problems for the institutions with a system that is also rife with data leaks and extremely detrimental to the consumer, and you have an expensive system to conduct identity verification that isn’t working well for anyone except bank regulators who are racking up the fines. It is time for a system that allows self-management of identity data by consumers and better standardization and mutualized costs for institutions. In addition, self-sovereign identity offers multiple opportunities for FIs to turn their KYC-shops into a revenue generator rather than a cost center. There will always be a need for a signing authority to credentialize a new user at the beginning of the self-sovereign identity process. FIs are well-equipped to provide this service with

their existing KYC departments and, in fact, in some countries are already the preferred method to establish identity for an individual. With self-sovereign identity, FIs can receive a fee from the network for conducting this service on behalf of the network as a whole, who now no longer needs to conduct the KYC process on their own. This concept works best with a consortium model of mutually trusting organizations, all working off a standard credential and KYC concept.

Footnotes

1. *Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity*, Thomson Reuters (May 9, 2016), https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html. ↩
2. *AML, KYC and Sanctions Fines for Global Financial Institutions Top $36 Billion Since Financial Crisis*, PR Newswire (Jan 29, 2020 6:00 PM), https://www.prnewswire.com/news-releases/aml-kyc-and-sanctions-fines-for-global-financial-institutions-top-36-billion-since-financial-crisis-300994923.html. ↩
3. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. ↩
4. Ben Wolford, *A Guide to GDPR Data Privacy Requirements*, GDPR.eu, https://gdpr.eu/data-privacy/ (last accessed Feb. 23, 2021). ↩
5. Allen C., *The Path to Self-Sovereign Identity,* Life With Alacrity, (Apr. 25, 2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html [hereinafter *Path to Self-Sovereign Identity*]. ↩
6. *See*, Margie Cheesman. *Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity,* Geopolitics 11. (2020) at 7; ("All of the distributed nodes within a network share the same consensus algorithm. These are designed to allow transactions to be completed and information to be synced, even if the actors in the network do not trust each other"); *See also*, Krause, Solvej Karla; Natarajan, Harish; Gradstein, Helen Luskin. *Distributed Ledger Technology (DLT) and blockchain.* FinTech note: 1 Washington, D.C., World Bank Group. (2017)

http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain. ↩

7. *But see e.g.*, Walch, A., *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems* (January 30, 2019). Crypto Assets: Legal and Monetary Perspectives. ↩

8. *See* Figure 1, Layer 1. ↩

9. Blockchain Records and Transactions Act of 2020, H.R. 8524, 116th Congress (2019-2020). ↩

10. *Id.* ↩

11. *Id.* ↩

12. Dirk Zetzsche, Ross Buckley and Doughlas Arner, *The Distributed Liability of Distributed Ledger: Legal Risks of Blockchain*, 52 University of New South Wales Faculty of Law Research Series 1, 16-18 (2017). ↩

13. *Id. at 16.* ↩

14. *Id.* at 15. ↩

15. Marcos Allende Lopez, *The Future of Identity: Self-Sovereignty, Digital Wallets and Blockchain*, Inter-American Development Bank (2020), https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf. ↩

16. Improving Digital Identity Act of 2020, H.R. 8215, 116th Congress (2019-2020). ↩

17. *Id.* ↩

18. *Id.* ↩

19. *Id.* ↩

20. *Id.* ↩

21. Zetzsche, Buckley and Arner, *supra* note 10 at 1. ↩

22. John Salmon and Gordon Myers, *Blockchain and Associated Legal Issues for Emerging Markets*, Emerging Markets Compass 1 (2019),

https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F. ↩

23. *Id* at 2. ↩
24. Zetzsche, Buckley and Arner, *supra* note 10 at 20. ↩
25. *Id.* at 20-21. ↩
26. Salmon and Myers, *supra* note 20 at 2. ↩
27. *Id.* ↩
28. *See* Figure 1, Layer 2. ↩
29. *See* Figure 1, Layer 3. ↩
30. *See generally KYC/AML Data Solutions, 2020*, Chartis Research (2020), https://rdc.com/wp-content/uploads/2020/05/Chartis-Research-KYC_AML-Data-Solutions-2020-Market-and-Vendor-Lanscape-Report.pdf. ↩
31. Alfred Ng, *How the Equifax Hack Happened, and What Still Needs to Be Done*, cnet (Sept. 7, 2018 at 4:54 AM), https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/. ↩
32. Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, *Notice of Proposed Rulemaking, Financial Crimes Enforcement Network of the U.S. Treasury Department* (Dec. 23, 2020), https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets. ↩
33. *Id.* ↩
34. Jose Parra Moyano and Omri Ross, *KYC Optimization Using Distributed Ledger Technology*, 59 Bus Inf Syst Eng 411, 411 (2017). ↩
35. *Id.* at 417. ↩
36. *Id.* at 415. ↩
37. *Id.* at 417. ↩

38. *See* Moyano and Ross, *supra* note 34 at 420. ↩
39. *Id.* at 422. ↩
40. *See* Cheesman M., *Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity,* Geopolitics 11. (2020) at 8. ↩
41. Zetzsche, Buckley and Arner, *supra* note 10 at 15. The authors of this paper note that decentralized identity protocols, specifically, the solution described in this paper, mitigates the risk of insider trading by not storing PII and related information on chain. However, of users select to use public DIDs rather than a pairwise approach, there is still a risk that PII or sensitive information coud leak. ↩
42. Emily Crane, *Regulation Without Deflation: Cryptocurrency and Its Insider Trading Conundrum*, 51 J.Marshall L. Rev 797, 802 (2018). ↩
43. Loi Luu, With Blockchain, Knowing Your Customer is More Important Than Ever, Forbes (May 17, 2018, 12:11 AM), https://www.forbes.com/sites/luuloi/2018/05/17/with-blockchain-knowing-your-customer-is-more-important-than-ever/#41c073ad559c. ↩
44. *Id.* ↩
45. Nikita Khateev, *Aries RFC 0037: Present Proof Protocol 1.0*, Github (May 28, 2019), https://github.com/hyperledger/aries-rfcs/tree/master/features/0037-present-proof. ↩
46. *Id.* ↩
47. *Id.* ↩
48. *Id.* ↩
49. *Id.* ↩
50. *See generally* Luu, *supra* note 36.. ↩
51. *See* Kevin Rutter, *If at First you Don't Succeed, Try a Decentralized KYC Platform: Will Blockchain Technology Give Corporate KYC a Second Chance?*, R3 Reports 6 (2018), https://www.r3.com/wp-content/uploads/2018/10/first_succeed_decentralized_R3.pdf. ↩
52. *Id.* at 5. ↩

53. *Id.* at 6. ↩
54. *Id* at 7. ↩
55. Lucas Mearian, *Amid privacy and security failures, digital IDs advance,* Computerworld (Jan 6, 2020, 3:00 AM), https://www.computerworld.com/article/3512108/frustration-over-growing-privacy-and-security-failures-advancing-self-sovereign-identities.html. ↩
56. Julie Dawson and Cristian Duda, *How Digital Identity Can Improve Lives in a Post-COVID-19 World*, World Economic Forum (Jan. 14, 2021), https://www.weforum.org/agenda/2021/01/davos-agenda-digital-identity-frameworks. ↩
57. Jayshree Pandya, *Nuances Of Aadhaar: India's Digital Identity, Identification System And ID*, Forbes (Jul. 16, 2019 at 1:00 AM), https://www.forbes.com/sites/cognitiveworld/2019/07/16/nuances-of-aadhaar-indias-digital-identity-identification-system-and-id/?sh=457f579d209d. ↩
58. Anviti Chaturvedi, *Overview of the Legal Issues around Aadhaar*, PRS India (June 10, 2017), https://www.prsindia.org/theprsblog/overview-legal-issues-around-aadhaar. ↩
59. *The Digital ID & Authentication Council of Canada Releases the Pan-Canadian Trust Framework Overview*, DIACC (Aug. 11, 2016), https://diacc.ca/2016/08/11/pctf-overview/. ↩
60. *Id.* ↩
61. Newly Launched Digital ID Framework to Begin Testing in Canada, DIACC (Sept. 15, 2020), https://diacc.ca/2020/09/15/newly-launched-digital-id-framework-to-begin-testing-in-canada/. ↩
62. *Id.* ↩
63. Trust Services and Electronic identification (eID), European Commission (Oct. 29, 2020), https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification. ↩
64. J.A., Ashiq, "The eIDAS Agenda: Innovation, Interoperability and Transparency," Cryptomathic. https://www.cryptomathic.com/news-events/blog/the-eidas-agenda-

innovation-interoperability-and-transparency. ↩

65. Shreya Ganguly, *President Approves Aadhaar Ordinance Allowing Private Cos to Access Aadhaar Info*, Inc 42 (March 14, 2019), https://inc42.com/buzz/president-approves-aadhaar-ordinance-allowing-private-cos-to-access-aadhaar-info/. ↩

66. Nehaa Chaudhari, Supreme Court has banned private companies from using Aadhaar. What does it actually mean?, Scroll.In (Oct. 4, 2018 at 10:30 AM), https://scroll.in/article/896771/supreme-court-has-banned-private-companies-from-using-aadhaar-what-does-it-actually-mean. ↩

67. *Id.* ↩

68. Simran Jalan, *Aadhaar Ordinance – Paving way for use of voluntary Aadhaar by Private Companies,* Vinod Kothari Consultants (March 15, 2019), http://vinodkothari.com/2019/03/aadhaar-ordinance-paving-way-for-use-of-voluntary-aadhaar-by-private-companies/. ↩

69. Dawson and Duda, *supra* note 49. ↩

70. "For example, it prohibits UIDAI and its officers from sharing a person's identity information and authentication records with anyone. It also forbids a person authenticating another person's identity from collecting or using their information without their consent.") Chaturvedi, *supra* note 51. ↩

71. Loïc Lesavre, Priam Varin, Peter Mell, Michael Davidson, and James Shook, A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems, National Institute for Standards and Technology 32 (2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf. ↩

72. *Id.* at 35. ↩

73. *Id.* at 32-35. ↩

74. *Id.* at 35. ↩

75. Scott J. Shackelford, Scott Russell, and Jeffrey Haut, Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks, 16 U.C. DAVIS BUS. L.J 217, 221 (2016). ↩

76. Nate Lord, *What is NIST Compliance?*, Digital Guardian (Oct. 7,2020), https://digitalguardian.com/blog/what-nist-compliance. ↩

77. *See id.* ↩
78. Martin Horan, *What is NIST? Understanding Why You Need to Comply*, FTP Today (May 22, 2019), https://www.ftptoday.com/blog/what-is-nist. ↩
79. *Id.* ↩
80. *See* Lord, *supra* note 69. ↩
81. *See* Lesavre, Varin, Mell, Davidson, and Shook, *supra* note 64 at ii. ↩
82. *See id.* ↩
83. *Id.* at 36. ↩
84. *Id.* at 40. ↩
85. *Id.* ↩
86. Lopez, *supra* note 13 at 44. ↩
87. *Id.* ↩
88. Sujata Tamang, *Decentralized Reputation Model and Trust Framework: Blockchain and Smart Contracts,* Uppsala Universitet 2-3 (2018), https://uu.diva-portal.org/smash/get/diva2:1352089/FULLTEXT01.pdf. ↩
89. Dawson and Duda, *supra* note 49. ↩
90. Naman Aggarwal, Wafa Ben-Hassine, and Raman Jit Singh Chima, *National Digital Identity Programmes: What's Next*, access now 26, (2018), https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf. ↩
91. *Id.* at 27. ↩
92. Dawson and Duda, *supra* note 49. ↩
93.

Julia Clarka, Mariana Dahana, Vyjayanti Desaia, Marta Iencob, Stephanie de Labriollec, Jean-Pierre

Pellestorc, Kyla Reidb, and Yolanda Varuhakic, *Digital Identity: Towards Shared*

Principles for Public and Private Sector Cooperation, GSMA, World Bank Group and the Secure Identity Alliance 33 (2016), http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf.↩

94. *Supra* note 83 at 24. ↩

95. Dawson and Duda, *supra* note 49. ↩

96. Ron Shevlin, *The 5 Hottest Technologies In Banking For 2020*, Forbes (Feb. 3, 2020 at 5:00 AM), https://www.forbes.com/sites/ronshevlin/2020/02/03/the-5-hottest-technologies-in-banking-for-2020/?sh=2f820232c0d3. ↩

97. Bank Fines 2020, Finbold (last updated Jan 11, 2021), https://finbold.com/bank-fines-2020/. ↩