

Customer Engagement for Utilities through Blockchain

Jay Malin, Ph.D.

AGENT511

425 Huehl Road #11B, Northbrook, IL 60062 USA

<https://www.linkedin.com/in/jaymalin/>

jmalin@agent511.com

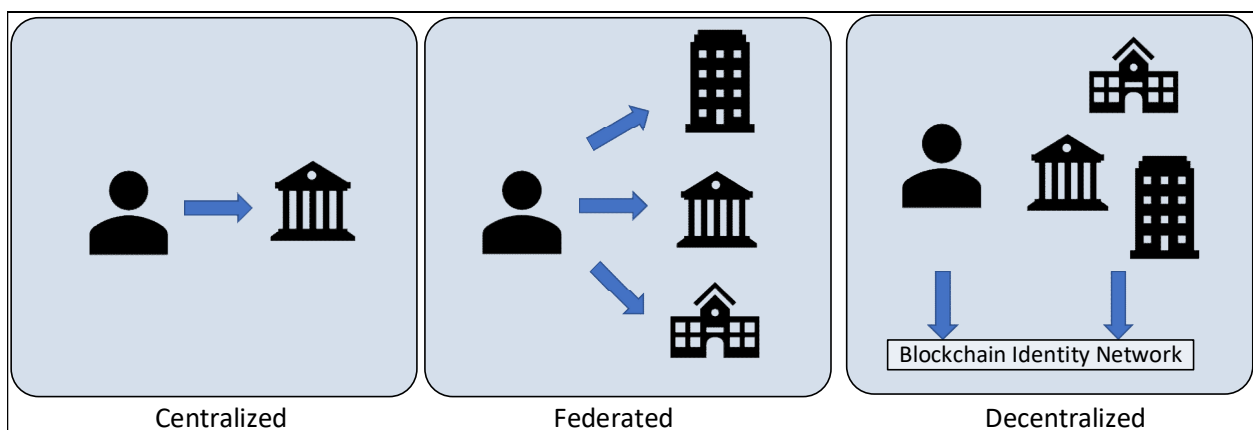
Identity landscape

Overview

For the utility to conduct its business, it is required to establish identity and create trust. At the time service is started, customers may be asked to prove credit worthiness, and as the relationship progresses, customers establish an online identity for the purpose of monitoring transactions. As the partnership between customer and utility flourishes, the customer may soon be an energy prosumer (buyer and supplier) or may acquire new services such as an electric vehicle (EV) loyalty program. The problem is that each transaction is encumbered by a barrage of clumsy requests for documents, email addresses, bank accounts, and security guarantees. Regrettably, this has the effect of slowing the pace of business at a time when most stakeholders are seeking technologies that encourage customer engagement and satisfaction and minimize the impediments to speedy, secure transactions.

Some organizations mistakenly believe they have resolved these issues by moving from a centralized identity model that has served them well for decades, to a federated model that leverages SSO and/or multifactor authentication. This only served to reduce the frustrating set of credentials required for the end user. Relieving the utility of the user authentication burden doesn't actually expand the business relationship. Until recently, despite numerous Internet breakthroughs, there was no single way to establish and verify identity except those shown on the left in Figure 1.

Figure 1: Burden of authentication across various forms of identity



Recent efforts to create Internet identity via the World Wide Web Consortium (W3C)¹, combined with advances in distributed ledger technology (DLT), commonly referred to as Blockchain, led to the realization of secure, immediate decentralized identifiers (DID). This form of identity is established by an

entity on the Internet and is memorialized on Blockchain. Essentially what DID does is allows any entity, whether individual, company, or device to establish a self-sovereign identity that is accessed by a secure digital key. DIDs contain pointers to identity proofs, verification methods, and service endpoints. The key—like an SSH key used to secure a server—is comprised of both private and public (sharable) keys that may be stored in computer memory or on a smart phone. The network also employs Decentralized Public Key Infrastructure (DPKI), which reduces the value of stealing user data.

The Sovrin Foundation is the leading decentralized identity network and is built upon a public, permissioned Blockchain called Hyperledger Indyⁱⁱ. SecureKey is one of the leading providers of decentralized identity solutions, including a smart phone application, Verified.me., that has been deployed in Canada as part of its Blockchain banking initiative. Other identity solution providers such as Credentia and Gemalto are built upon the R3 Corda permissioned Blockchain.

Countrywide identity example: Estonia

Currently, Estonia leads the digital identity frontier, primarily because of a mandatory national ID card and digital identity that facilitates citizen access to all of Estonia's e-services. This was implemented in order to overcome previous attempts to hack Estonia's centralized information systems. Estonia's successful implementation of a secure identity platform validates many of the purported benefits of deploying self-sovereign identity.ⁱⁱⁱ

Financial services identity example: CIBC (Canada)^{iv}

Numerous data breaches resulting in hijacked credentials, led the Canadian banking industry to implement a Blockchain identity platform that fulfilled the banking industry's need to know your customer (KYC). CIBC, along with other major Canadian banks, launched the Verified.Me service that enabled customers to create a decentralized identifier (DID) profile that associated their bank account attributes with their digital identity. Deploying Verified.Me digital identity offered the bank the ability to not only meet its KYC and anti-money laundering (AML) compliance standards, but as a way to improve customer convenience.






What comprises identity

Credential issuance

Currently, we are led to believe that our identity is confined to any one of the following: email address, social security, driver's license, and/or passport number, non-inclusively. Our utility defines us by a customer number which may be related to an account number, premise identifier, transformer, address, or node. Yet not one of these uniquely identifies us. Email address aside, they are simply identifiers that have been issued to us by credential service providers (CSP's). Our free email address is potentially held by a company such as Google, or even by our current Internet provider such as Comcast. By appending credentials to our decentralized identifier profile, we are able to securely identify ourselves to our utility. Our social security number is issued by the Department of Health & Human Services, and our driver's license issued by our State's Department of Motor Vehicles. Our credit report is tied to our digital identity as is our professional credentials such as education, work history, and professional certifications.

Moreover, so too is our utility account and premise address as verified by our utilities as shown in Figure 2 and the last panel in Figure 3.

Figure 2: my DID and credential relationships

 Me	Verifier: DHS Citizenship: USA Passport: 0123456 Issued: 9/19/19 	Verifier: Ameren Account: 012345678 Address: 123 Main St Issued: 8/5/18 Status: Active 	Verifier: Scrum Program: Master Issued: 5/15/18 
	Verifier: DHHS SSN: 012-345-6789 Issued: 8/5/70 	Verifier: Ameren EV Loyalty Account: 012345678 Vehicle: Tesla 3 Issued: 8/5/19 Status: Active Limit: \$50 	
	Verifier: UIUC Degree: BS School: EE Issued: 5/15/92 		

Some of this data, namely our address and transformer ID, may be in plain text on Blockchain, and other data which uniquely identifies us may be recorded “off-chain” by the CSP. What makes this secure, private, and immutable is the fact that this transaction is recorded on Blockchain and the relationship to our decentralized identity is encrypted. This means that no party can independently associate my credential on the Blockchain with my identity unless I have authorized them to do so. I can also specify how, and with whom, I want my credential shared. A couple of simple examples of this are:

- I can make my work experience publicly searchable and viewable on Blockchain, however, potential employers do not know my identity but may use features of my identity to contact me about a career opportunity.
- My credit score and annual income is stored with my identity and I wish to meet the utility’s credit worthy minimum requirements by showing that my FICO score is greater than 700 and my annual income is greater than \$50,000.
- I wish to take advantage of a discount for my town’s park district golf course but must verify local residence. I do so by sharing the address provided by my current utility service provider.

Digital identity has the democratizing effect in that no single government controls user identity, the user may share only the minimum required information needed with a verifier, and the user can remain anonymous, thereby avoiding discriminatory behaviors such as age, race, gender, and/ or religion.

Verifying Identity with Blockchain

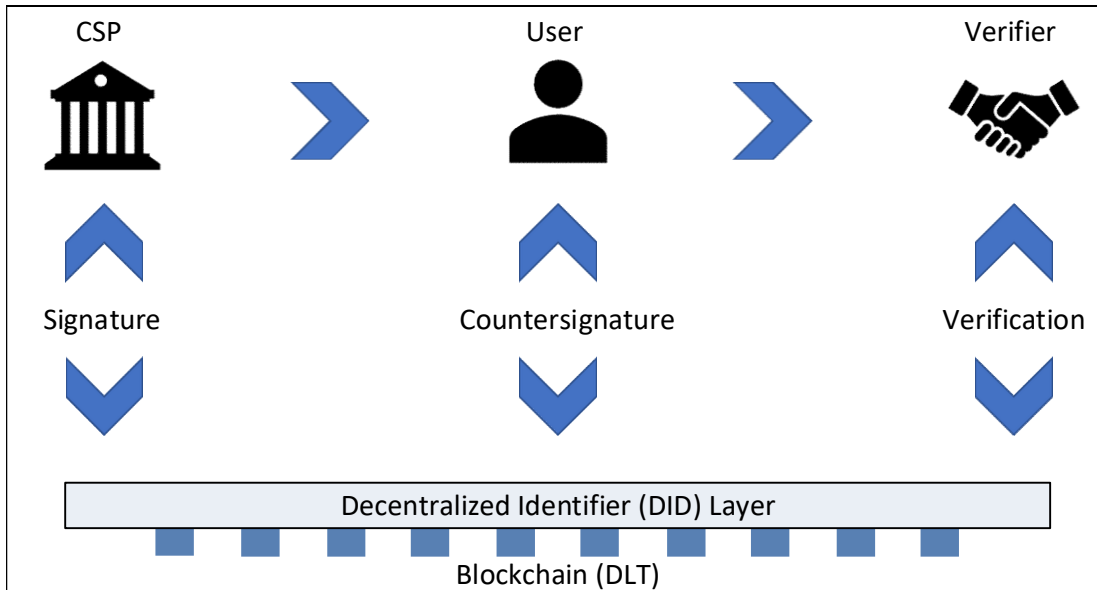
The user creates his/her identity with one of the aforementioned service providers, many of whom offer a digital identity wallet in order to store their attestations, like credential issuances. The wallet may be secured on the smart phone, as shown in the panels in Figure 3, using various forms of biometric and multifactor authentications. Example biometric authenticators include retina and facial scan, fingerprints, voice, and even DNA; not all of which independently are suitable to uniquely identify an individual. The wallet is initially empty until a variety of authoritative sources and attestations are added such as government identifications, education and professional development, and credit agencies and service providers.

Figure 3: Digital identity wallet examples



As shown in Figure 4 below, a user has a blockchain digital wallet (at the bottom of the figure). An issuer issues an attestation or claim (e.g. a birth certificate) to that user. The user countersigns the attestation (birth certificate), accepting it into their wallet. When the verifier wishes to validate the user's date of birth, the user presents the birth certificate to that verifier. The verifier uses the blockchain to verify that the birth certificate was issued by a valid issuer and hasn't been revoked or altered in any way.

Figure 4: How Attestations are Created and Verified



How Does Blockchain Transform Identity?

Blockchain technologies transform the identity lifecycle several ways:

- **Reduces identity fraud** by prohibiting the counterfeiting and misuse of digital identity credentials across the blockchain network. With blockchain, provenance is assured since each credential is linked back to the issuer. When paired with improvements in biometric technology, DID's allow near-certain probability of authenticity.
- **Reduces risk of data breaches** by distributing information among counterparties. Due to the advantages of blockchain architecture, a single attack will not yield significant returns, thereby minimizing the likelihood of a severe database compromise.
- **Reduces redundancy** by allowing the credential issuer to have to attest to a credential only once. With blockchain, verifiers can validate address and utility relationship instantly, without having to contact the credential issuer, in this case the utility, directly each time.
- **Increases privacy** for end users when sharing personal data. Given the correct architecture, a decentralized identity system offers end users more control and discretion over their data, enabling them to share only what they need or want to share.

Blockchain & Utility Customer Engagement

Start of service

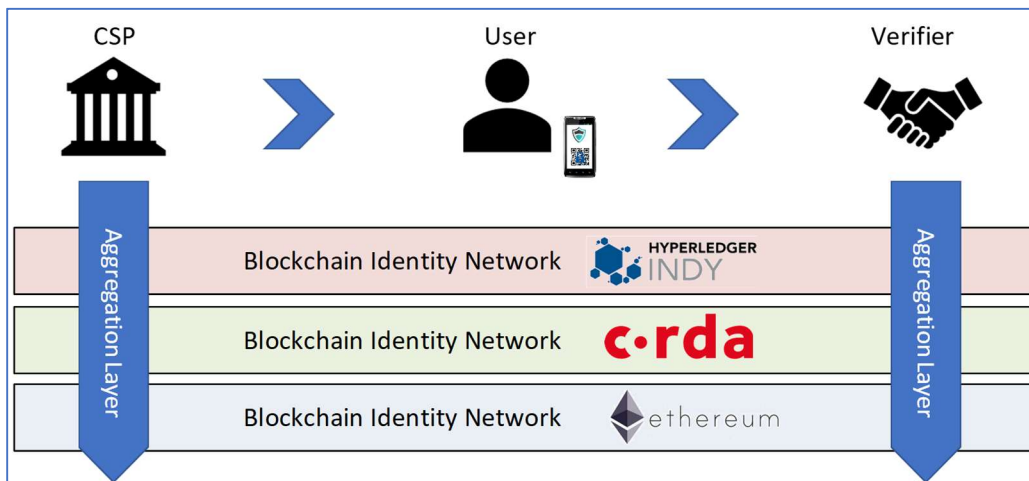
Typically, the start of new service is a cumbersome, time-intensive, and interactive process by which the customer provides various forms of identity and credit worthiness. The customer may be asked to provide their social security number, previous addresses, other forms of credit guarantees, and contact information. This process is carried out over the phone with a Customer Service Representative (CSR) or on-line. Some efforts are underway to simplify flows for existing account transfers using interactive voice recognition (IVR) and web forms. Major utilities undergo a process, sometimes called the "Name Game", to further discern customers with similar names, especially if credit worthiness is questionable.

As shown in Figure 5, customers need only share their decentralized identity by selecting their decentralized identity service provider. Once the provider has been selected, the individual accesses their key to authorize and share only the necessary data that defines identity and credit worthiness. Once the process is fully completed, the utility is now also able to attest that the customer's identity includes a utility account credential as shown on the left of Figure 3.

Figure 5: sample utility start service page

While this could conceivably require the utility to integrate its customer information system (CIS) with all DID networks, we propose herein a new layer that essentially extracts the complexity out the process by aggregating the DID networks. This aggregation platform would be publicly available and would offer a simple JSON integration model that relieves credential service providers and verifiers (such as the utility), of the burden of integrating with each identity network as shown in Figure 6. Note in this utility example, the utility is both the CSP and the verifier.

Figure 6: Identity aggregation and integration layer



Utility preference management

Once the account is started, customers may login using their digital identity keys, thereby avoiding the frustration of creating yet another username and password. Thereafter, digital identity may be used to quickly and easily authenticate mobile apps and allow the utility to issue additional credentials to users

such as energy conservation awards and verified participation in an EV loyalty program. Digital identity then becomes a natural extension of customer preference tools; whereby customer contacts, language preferences, and program participation is inherently tied to their digital identity. As an example, a customer wishing to purchase EV energy on their home (ComEd) or a guest (Ameren) network, need only furnish their identity with the applicable loyalty program credential. This may be compared to the way in which wireless users roam to other networks but are identified by their SIM cards. In the case of the latter, the guest network must clear the transaction with the user's home network. With digital identity and Blockchain, EV users can be identified and the transaction may be cleared immediately (or at minimum, the home energy provider is verified in real-time).^v

Digital identity may be used to quickly create a payment wallet. When combined with Blockchain coins and tokens, bill payment, energy trading credits, and even DER, instant and potentially anonymous payment for energy is realized.

Additionally, within Blockchain identity, there is a new concept spearheaded by the Sovrin Foundation, called tokens, which allows stakeholders in the Blockchain ecosystem to pay for the burden of identity maintenance. A utility may pay for a credit check and identity verification using a Sovrin tokens (monetized on the Blockchain's exchange) and the utility may be paid for its ability to verify a customer's address or green status.

Energy credits

An energy prosumer can deliver value to the utility by purchasing energy and providing surplus energy. Distributed Energy Response (DER) generation is delivered by a combination of solar, wind, or battery—and in some cases, the DER unit may not be a current customer but a source wishing to remain anonymous. The source may also maintain a digital identity to which the utility pays for each unit of energy – a Kilowatt hour or Therm – with a Sovrin token. Tax authorities are notified of the transaction by shared tax identity credentials. There are several other references about using Blockchain to trade energy; the key differentiator is the ability to use digital identity to define the participants in the transaction.^{vi}

Adoption of Distributed Digital Identities

Digital identity standards are now starting to mature; however, it is recommended that utilities stay on top of the various decentralized identity standards (W3C, NIST, IETF) and review research such as Gartner^{vii} and Energy Central's publications or leverage consulting services similar to AGENT511's. Because digital identity is even more meaningful when leveraged by credential service providers, it is recommended that utilities form alliances with federal, state, and local governments, other utilities, local banks, and credit agencies. Some identity platforms publish SDK's and our company, AGENT511, is documenting an integration model for its aggregation engine.

Blockchain platforms enable the interaction of citizens, credential issuers, and credential verifiers while ensuring access to the credentials of a citizen will remain private based upon the requirements of the application.

Given the degree to which identity infrastructure is embedded in our daily lives, the adoption of digital identity and Blockchain will likely be gradual and the emergence of an industry standard may take time.

As a result, industry should look to leverage platforms that aggregate and abstract the complexity of varying standards and platforms versus waiting for large-scale adoption or attempted standardization.

To encourage participation and discourage the evolution of new siloed systems, an additional layer is required to ensure the evolving systems can communicate. The aggregation concept anticipates an individual-centric model, where citizens select a digital identity and blockchain platform of their choice. The verifier, must then be able to interact with multiple platforms. This platform-level interoperability is the aggregation concept.

Regulation and Compliance

The direction of personal data privacy policy favors decentralized identity. Current legislative trends favor concepts such as the right to be forgotten and GDPR. For enterprises, the inherent framework of decentralized identity and blockchain technologies facilitate compliance with stringent regulations that emphasize privacy and transparency; all of which are barriers for today's centralized identity systems. Additionally, this approach provides individuals an opportunity to dynamically update personal data so that relying parties always have current information.

While compliance with new legislation is key for adoption, decentralized identity and the associated standards similarly to World Wide Web Consortium and NIST 800-63^{viii} are still developing.

Summary

Privacy and security are major priorities for large organizations and utilities are no exception. Current approaches, including Federated identity models, fail to solve these problems and further limit innovation across the utility. By leveraging self-sovereign identity and unlocking the potential in blockchain, utilities are able to tap unrealized opportunities in service delivery, EV loyalty and mobility, and energy credits and DER programs. Digital identity encourages customer engagement and mitigates barriers such as the rapid user authentication required to facilitate customer participation in new revenue-generating programs. While digital identity standards and platform service providers are evolving, utilities can take advantage of aggregation platforms that help to mitigate the complexity associated with integrating into numerous identity networks.

ⁱ <https://w3c-ccg.github.io/did-spec/>

ⁱⁱ <https://sovrin.org/library/sovrin-protocol-and-token-white-paper/>

ⁱⁱⁱ [Estonian citizen but provides digital access to all of Estonia's e-services](#)

^{iv} <https://www.itworldcanada.com/article/canadas-big-5-banks-launch-blockchain-based-digital-identity-service-with-securekey/417406>

^v <https://www.accenture.com/us-en/insights/utilities/beyond-the-blockchain-buzz>

^{vi} <https://www.sciencedirect.com/science/article/pii/S1364032118307184>

^{vii} <https://www.gartner.com/en/information-technology/insights/blockchain>

^{viii} <https://csrc.nist.gov/publications/detail/sp/800-63/3/final>