DECENTRALIZED IDENTITY FOR BANKS

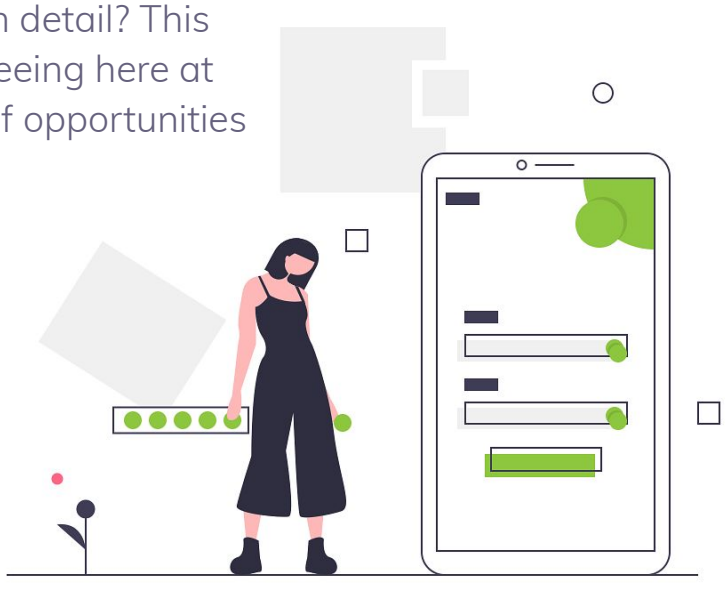
evernym

Introduction

The financial world is grappling with requirements to be more controlled (regulated), and yet more flexible to the real-time 24/7 expectations of customers. Responding traditionally is just creating more technical and operational complexity and cost. Banks need to break the cycles of change and increasing complexity, and they need the tools to do so.

Evernym's very first customer was a global bank, that foresaw the value of an open protocol for digital identity "way back" in 2016 (eons in the world of blockchain tech). We helped them to understand and demonstrate how this new technology could fit into traditional banking practices. Since then, we have seen increasing interest from the financial services sector around the world, and it continues to be the most active of all the customer types we work with.

Why is everyone getting excited and spending valuable and scarce resources examining this new technology in such detail? This whitepaper will outline what we are seeing here at Evernym, and describe the spectrum of opportunities that are on offer.



But first, what is decentralized identity?

Decentralized or "self-sovereign" identity can appear very complex, involving lots of new terminology and exotic cryptography. Add in misconceptions, misunderstandings, and misinformation from incumbents protecting their positions, and it's easy to see why it can be hard to get a grip of.

In reality, it's really simple. People will carry verifiable digital equivalents of the paper and plastic documents ("**credentials**") they have today, issued by the same organizations and authorities. They will be able to control whom they share them with and when they share them, just like you can with paper and plastic today. But unlike paper and plastic, these digital credentials come with cryptographic superpowers that preserve privacy and enable instant verification of their authenticity.

Decentralized identity has two components:

1. **A standard, open protocol for issuing, holding and verifying digital credentials**, like driving licenses and membership cards. A bit like SMTP or TCP/IP protocols that make email and the internet work everywhere. Anyone can build on to of this protocol.

2. **Somewhere to store the verification keys of credential issuers**, that allows anyone to locate and retrieve them at any time to verify any attribute that adheres to the protocol. While this could be any database, it is important to ensure there's no backdoor, no admin access, and no reliance on a single monopolistic provider. Therefore, a decentralized distributed ledger is an ideal storage medium, especially one like Sovrin which has been designed for this purpose.

By combining these two components, digital identity is transformed. Everyone everywhere can issue, hold, and verify any credentials about anything. No more proprietary silos "owning" your identity. And the same protocol and store can be used for people, organizations, and things. **You finally get increased security and reduced friction**. It all seems so obvious and simple.

& What decentralized identity is *not*:

Decentralized identity may appear to be a panacea, a cure for all manner of horrendous problems, but it doesn't work in some scenarios:

- **It doesn't work for blacklists such as no-fly lists, or politically exposed persons (PEP) and sanctions lists**. People don't go around with a piece of paper saying they are on a sanctions list now; and if they did, you couldn't force them to produce it. The digital world is no different. Blacklist checks will still be needed.
- **It doesn't mean everyone "self-attests" all the information about themselves**, removing the need for governments. Just like with paper and plastic, you will need human trust in the issuers of the credentials and their onboarding processes.

Also, decentralized identity is **not a replacement for civil registers** like driving license authorities, passport issuers, and birth registries. They are still vital. All that will change is that, when they issue you a paper or plastic certificate/license, they'll issue you a digital one as well.

And lastly, decentralized identity is **not a "rip and replace"** for all existing identity schemes and systems. We will see an evolution, where existing systems are *enhanced* to issue and verify digital credentials.

Why are banks interested?

We're seeing three main drivers of interest in decentralized identity for banks:

1. KYC and AML cost reduction.
2. Customer experience improvements.
3. Compliance with new privacy regulations.

1. Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) cost reduction

Banks suffer from very high regulatory costs, highly complex procedures, and massive penalties for failure to comply. According to Forbes, major banks spend up to **$500 million** USD each year each, with **$25 billion** being spent in the USA on AML compliance. The fines in the USA for non-compliance have topped **$24 billion** since 2008.

These are astonishing amounts of money. It's painful and expensive. And it kills customer experience. The same Forbes article states that on average it takes 24 days to complete the customer onboarding process.

If you thought individual KYC is expensive, corporate KYC is horrendous. Having to track down the ultimate beneficial owner of a multinational organization can take months and cost many thousands of dollars. It's so expensive because there is no standard protocol for proving corporate or individual identity.

Therefore, it's not surprising that there is strong interest from banks in a solution that provides **virtually instant verification of customer data**. Anywhere there is a huge cost, there will be innovation targeted at reducing that cost, and that's a primary driver of the interest we are seeing.

2. Customer experience improvements

Another key driver is the customer experience. There has always been a compromise between high security and frictionless customer experience. It's always been one or the other, not both.

That is changing, as it becomes possible for customers to sign up or login with just one or two clicks, using authentic and instantly verifiable identity data. No more forms, no more usernames, and no more passwords. Just trusted digital credentials. Our bank customers are targeting onboarding times of a few seconds, not hours or days.

This transformation of customer experience won't be limited to banks. It will cover the whole spectrum including retailers, airlines, employers, and so on. **Anywhere that forms and passwords and back-office checks exist will be revolutionized.**

3. Compliance with new privacy regulations

Regulations such as the GDPR are putting pressure on banks to collect less data, when they are also required by other regulations to collect more of it.

In the new world, verifiably authentic data will come directly from customers, with an audit trail. And the advanced cryptography now available will mean that only the data required to execute a transaction is needed, rather than the current practice of over-collecting data that is not immediately relevant.

Additionally, because of the way that decentralized identity works, a bank will have **a persistent, secure, and unique connection** with each of its customers. This means that the bank can re-request data to satisfy periodic checks, and it is quick and easy for the customer to respond.

As an additional bonus, this secure connection can also be used to send any other information to and fro, such as statements, loan documents, and address changes, as both parties are able to verify who the other is.

What are the opportunities facing banks?

Banks pride themselves on being bastions of trust. As digital identity evolves, banks are very well placed to stretch from trust for money into trust for identity.

The easiest way to look at how banks can get involved is to use a spectrum, from doing nothing to going all in on decentralized identity for banks. Below is a sample of that spectrum with some of the ideas and projects we are working on with customers right now:

1. Do nothing.

Wait for other banks and see what happens. Financial institutions have already started. Regulators are involved. The pathfinders are already building a significant competitive advantage. Once they can onboard a genuine customer in 5 seconds, how will you catch up?

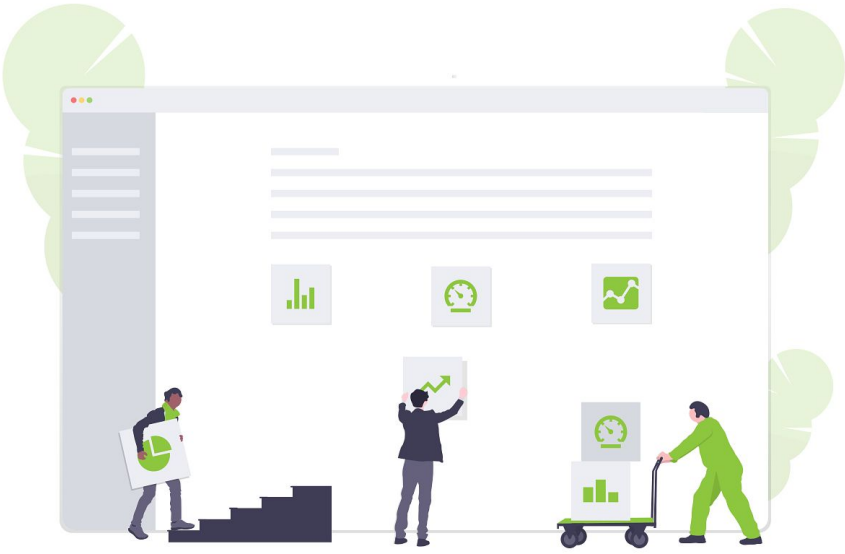
2. Issue credentials to your own customers, for use within your own bank.

Increase security and convenience by providing your customers with a verifiable credential proving that they are a trusted customer, that they can use whenever they call in, walk in, or log in. Example – US credit unions led by the CULedger initiative.

3. Cross internal silos.

This is a simple extension of the above opportunity. Once a bank enables the customer to digitally prove they are a customer, that customer can be the courier of that information across a bank's own internal silos.

This means that all those hugely expensive database integration projects and single customer view projects can finally finish. You don't need to build increasingly large and toxic data lakes. You can "outsource" the "single view of the customer" to each customer.



4. Build 1-1 secure connections with every customer.

One benefit of the open credential exchange protocol is that a bank will have a 1-1 secure, private connection with each individual customer.

It's like you have a separate VPN with each customer. You know it's the customer, and the customer knows it's their bank. Over this connection, you can send statements, chat 1-1, request identity data, send offers, onboard for new services, etc.

5. Transform new customer onboarding into a 1-click experience by accepting credentials from other issuers.

As the ecosystem of digital credential issuers grows, banks will find new customers coming to them who already have trustworthy credentials issued by other parties that the bank already trusts, like telcos, utility companies, identity providers, and government bodies.

Banks will be able to verify their data in seconds and onboard these new customers with minimal friction.

This has already started. Evernym is working with Deloitte (which has a customer onboarding solution), Onfido (which carries out digital identity checks for thousands of organizations around the world), a number of banks, and the UK regulator, the Financial Conduct Authority.

Banks can play a massive part in stimulating this new ecosystem.

6. Minimize collected data and provide a verifiable audit trail.

When a customer is onboarded using verifiable credentials, the protocol allows for the collection of just the minimum data required to execute the onboarding transaction. For example, rather than getting every attribute from a driving license, most of which are unnecessary to open a bank account, the bank can ask for just the relevant attributes.

This is called "**selective disclosure**," and it enables a bank to demonstrate that it is only collecting the data required. It is built into the credential exchange protocol – you can use it right now.

The data comes directly from the customer, with their consent, and the bank can prove to a regulator when and from whom it received the data, as well as the authenticity of the data which it will have verified using Sovrin. The customer will have a corresponding record of the data that they sent.

7. Be "top of wallet" – the Identity Wallet.

Digital credentials are kept in "wallets," just like paper or plastic credentials are, but with **higher security** and **better protection against being lost or stolen**.

One benefit of standardized digital credentials is that they can be used anywhere in the world. Just like paper but with cryptographic superpowers.

The bank that issues useful credentials that help customers in their broader digital life will rapidly find themselves at the top of their customers' identity wallets.

Just like standardized credit cards that let people spend anywhere, providing customers with a digital credential that they can use anywhere in their digital life to prove age, address, or financial status will be the gateway to seamless, trusted digital services for the customer with retailers, airlines, public services, etc.

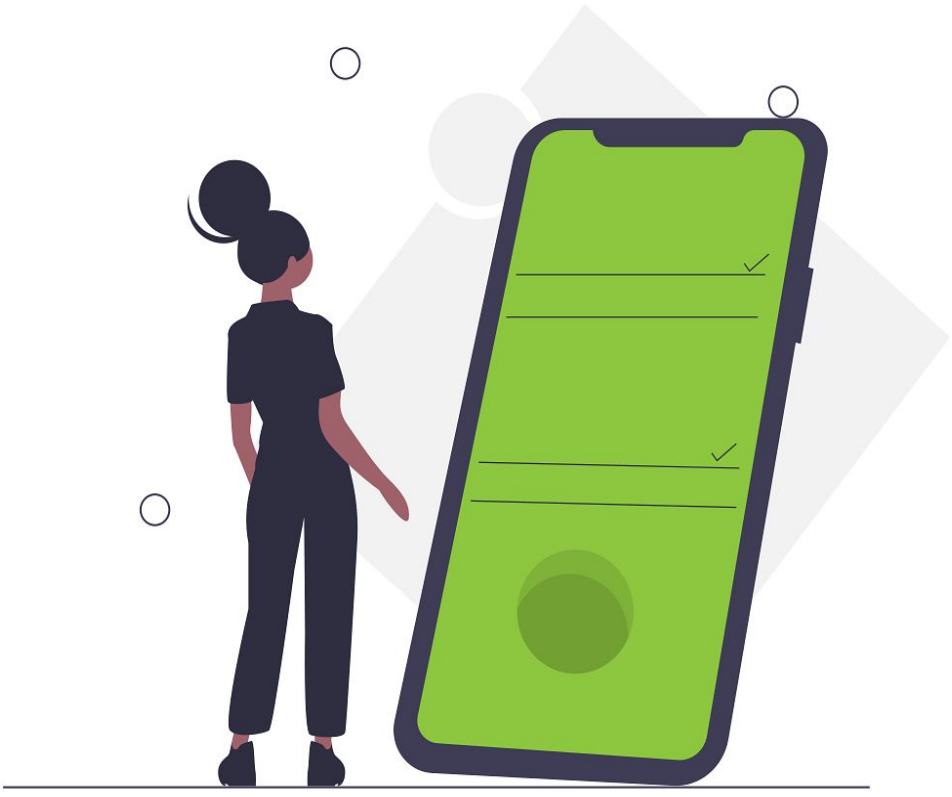
8. Provide customers with an identity wallet.

There will be an open market for developers of the digital wallets that are used to hold these new digital credentials. Due to open standards, the credentials and the wallet that contain them do not have to come from the same source.

Banks already have secure apps that their customers use. It makes a lot of sense to build credential wallets into these apps.

Evernym created the first Sovrin-compatible wallet to be released into the Apple and Google app stores, and we're already working with a US financial institution to provide a wallet SDK to build into 3rd party apps for exactly this purpose.

There are some drawbacks with this approach though. It might seem weird to open your bank app to prove you are a doctor, for example. And if you have numerous apps with credential wallets built in, which is the primary one that notifies you of a proof request, and how do they stay in sync? These are some of the issues being worked on already in the Hyperledger Community, and one of the reasons behind the spin-off of Hyperledger Aries from the main Hyperledger Indy codebase.

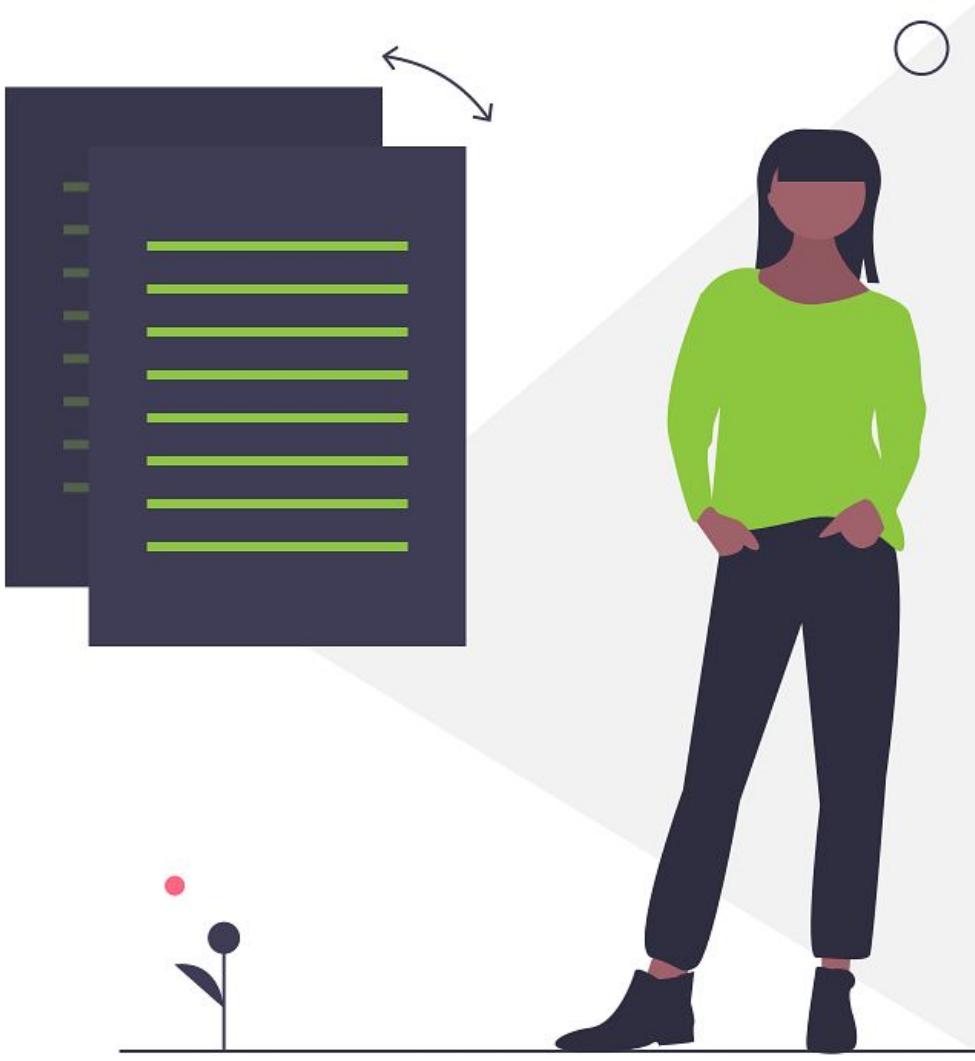


9. Help customers with backup and recovery.

Unlike physical credentials, digital credentials can be backed up and recovered in the case of loss.

Every credential wallet needs a backup component. Evernym's Connect.Me wallet already provides the ability to securely backup and restore your credentials in several ways. Backup is great, but the important bit is the secure storage of the backup and its recovery, should that be necessary.

Banks can play an important role by providing a "**safety deposit box**" for backups and helping people to recover their backup by adding additional layers of security to the process.



10. Be the safety deposit box for customer credentials.

There will be customers who need more help than just backup and recovery of credential wallets.

Some customers may want their bank to hold their digital credentials and keys for them. This is a concept termed "**guardianship**." As with many things in this new decentralized identity world, it's analogous to the physical world where I may put some share certificates or other valuables in a bank's safety deposit box.

Importantly, digital credentials are portable. Just like my share certificates or valuables, I can take my credentials out of my bank and go and put them in another bank. This new world has no lock-in. Banks will need to compete to provide the best service.

Guardianship is not limited to banks. It applies in many other arenas as well, such as for refugees who have nothing and need an NGO to help them get started with a digital identity, or an elderly relative who is unable to act on their own, or a newborn baby. In fact, all the scenarios that apply in the world of physical credentials apply to the digital world as well.

Guardianship is not limited to people. Animals, connected things, and corporations all have human guardians and controllers.

As you might expect by now, there is already work underway to define the role of guardians and how they technically operate. You can look at this further by finding "Guardian" in the Sovrin Glossary.

Most of the suggestions above have focused on human credentials. Organizations can have credentials as well. In Canada, the provinces of British Columbia and Ontario have already issued millions of organizational credentials using the live Sovrin network.

The transformative effect of organizations having verifiable digital credentials will be immense. We have just started to scratch the surface. Novartis, for example, has demonstrated how they can issue digital credentials to their supplier organizations so that they can be verified instantly at any Novartis site around the world.

Conclusion

The breadth and opportunity that open, standardized digital credentials offer the world is so large it's almost impossible to envisage. Every digital interaction involves identity of some kind. That is the scale and scope in front of us.

For banks, the opportunity to finally have **higher security** AND **less friction** is now here. Finally.

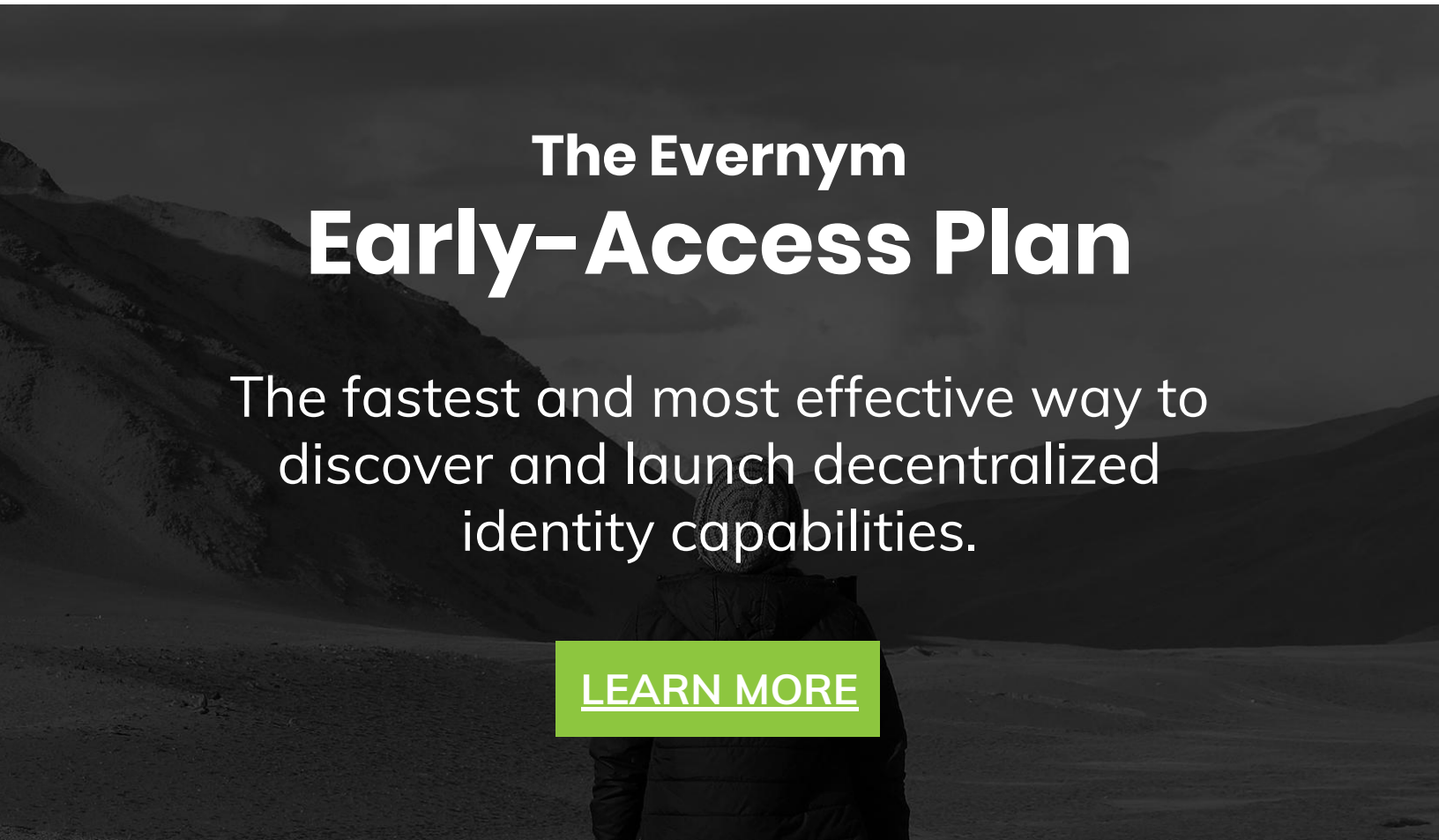
By cutting out the middle-man and returning to trusted point-to-point relationships, things become a lot simpler. Advances in cryptography and decentralization open up a host of new possibilities across the banking spectrum.

Banks are very well positioned to provide a range of attractive new services to customers that save money and create new business opportunities. Those that move fast will gain considerable competitive advantage.

The first step is to do something for themselves, in their own ecosystem. This could be it cross-silo authentication or secure call-in, walk-in, and log-in, or solutions for anywhere that customer consent is needed for transaction approval.

The beauty of an open standard approach is that there is effortless portability. Become an issuer of credentials for your customers. Help their digital lives to become more secure. They'll love you for it. And as others issue credentials, you'll be able to onboard new customers quicker, and more securely than ever before.

If you want to know more and get started, Evernym is here to help.



About the authors

Andrew Tobin

VP Delivery, Evernym

Andrew is a technology strategist. He has a history of delivering innovative technology solutions to complex business problems in the converging worlds of banking, mobile, and identity markets. He has built payment networks, created a mobile bank, run a £billion mobile messaging platform, and been deeply involved in the design and creation of self-sovereign identity network Sovrin and its underlying Hyperledger Indy technology.

Jo Spencer

Champion, 460degrees

Originally a research scientist, Jo fell into designing and building payments systems across the globe 29 years ago for Logica in London. These systems ranged from infrastructures for countries, securities and FX settlement systems, to solutions and products for banks. For the last 10 years, Jo was the Head of Technology, Strategy and Architecture at the ANZ Bank based in Melbourne and was central to the design and implementation of the real-time New Payment Platform in Australia. Jo's frustration with unnecessary friction in the payments process led him to advocate the Self-Sovereign Identity model for payments and all sorts of other cool applications. Now, as a Champion with the 460degrees Expert Management Agency, Jo provides guidance to a long list of happy clients across Australasia.