Digital Identity and Blockchain:

Opportunities and Challenges for Financial Institutions

Vijayakumar Thirugnanasambandan CAMS-Audit, PMP
Table of Contents

Executive Summary .................................................................................................................. 3
Digital Identity ........................................................................................................................ 4
Blockchain: Distributed Ledger Technology (DLT) .................................................................. 5
Uses and Success Stories of Blockchain .................................................................................. 7
Advantages of Blockchain ....................................................................................................... 7
How Blockchain Can Resolve Digital Identity Issues ............................................................. 8
Blockchain and Digital Identity Programs In-flight ................................................................. 9
Blockchain-Based Digital Identity Initiatives by Banks .......................................................... 10
Advantages for Banks in Being Part of a Blockchain Digital Identity Network ....................... 11
Opportunities for Banks in This Space ................................................................................... 12
Challenges for Banks in Adopting Blockchain ....................................................................... 12
Impact of Blockchain on Audit and Assurance Process ......................................................... 13
Conclusion ............................................................................................................................. 14
References .............................................................................................................................. 15
Executive Summary:

“On the Internet, nobody knows you’re a dog” was a famous *New Yorker* cartoon first published in 1993, and, despite 25 years of technological advances, the saying remains true. Digital identity is one of the Internet’s oldest and most challenging problems. (1)

In the real world, we use physical credentials, such as national IDs, passports, or driver’s licenses, which are issued by a trusted authority, to prove our identities to another human being or company.

In the online world, we don’t have an equivalent to physical credentials to prove our identities; instead, we use tens or even hundreds of usernames and passwords. Our personal details are all over the place across several different databases and guarded by companies that may not have the capability to keep them safe.

This wave of digitization is influencing every facet of human life and spreading at an exponential rate. The increased use of online platforms, including social media channels for accessing financial services, has led to a huge rise in cybercrime. We see instances of email accounts, network passwords, and credit card details becoming compromised. Digital identity and knowing your customer (KYC) is top of mind for financial institutions (FIs) facing cybersecurity threats (2).

Traditional identity systems are costly, fragmented, and are not robust enough to face sophisticated attacks, and this limits financial institutions in providing a seamless transaction experience.
Digital Identity and Blockchain

A digital identity solution based on blockchain, or distributed ledger technology (DLT), is economical, immutable, secure, easily accessible, and provides a legitimate audit trail (3).

This white paper addresses:
- The opportunities for FIs that come from adopting a blockchain digital identity solution to reduce KYC costs, tap into new markets, and improve their core financial services
- The challenges that FIs must address in order to make the blockchain adoption viable and scalable from an implementation, control, and monitoring perspective
- The impact of blockchain on audit and assurance processes

Digital Identity

What is digital identity?

A digital identity is the body of information about an individual, organization, or electronic device that exists online (4).

The need for digital identity (5)

Customers are expecting more convenient real-time, mobile-first, and seamless experiences. At the same time, data breaches hitting the headlines increase concerns about data privacy.

It has become clear that the growth of online business and banking requires strong and reliable digital identity solutions, which allow new players and incumbents both from the public and private sector to authenticate, identify, and operate in a safe and efficient way with the latest technologies, such as biometrics, blockchains, and artificial intelligence (AI).

The regulators are taking an increasingly active role. In the EU, for example, the General Data Protection Regulation (GDPR) already includes eIDAS (electronic Identification Authentication and Trust Services). Compliance will also start to demand robust data protection, privacy, and control for customers.

Current issues and challenges in digital identity

One of the key problems in cyberspace is knowing with whom one is interacting. Based on a human’s judgement and basic verification procedures, it is relatively easy to verify a paper identity document. However, when it appears online, there is no human on the other end of the Internet connection; rather, we have a machine and digital credentials to validate. (1)

Validating a digital credential requires solving two problems:
1. Standardizing the format
2. Standardizing the way to verify the source and integrity of the digital credentials

Current state and problems (1)

Digital signatures as forms of ID are legally valid in many jurisdictions around the world. The digital signature requires two keys: the first is the private key, or “signing key,” which is used to sign the document and is kept secret by the issuer; the second is the public key, or “verification key,” which is used to verify the signature and make sure the digital credential is not tampered with. This one need not be kept secret.
Digital Identity and Blockchain

The problem is, there should be a standard way to verify the public key of the issuer to prove the authenticity of the credential. The usual answer to this problem is to have a public key infrastructure (PKI).

The basis of public key cryptography is that anyone can verify the digital credential with access to the issuer’s public key. Each private key has only one public key, and vice versa. Both the public key and private key are cryptographically connected.

The basic problem with PKI is that it is cumbersome, costly, and centralized. The public key certificates are issued by certificate authorities (CAs) who are only in small numbers. To get a certificate from CAs takes time and effort. This is hard for individuals to deal with; hence, these are mostly purchased by companies. Moreover, introducing a middleman (the CA) into our digital trust infrastructure is a vulnerability. The CA could have made a mistake in the digital certificate, their service may go down, they may increase the price, or may go out of business—this causes the whole system to fall apart. Centralization of this nature can lead to single points of failure.

A better way to manage digital identity is required.

Standards for digital identity (6)

ISO has established technical committees, subcommittees, and working groups that are in continuous communication with other international and national organizations, as well as industry consortia involved in reviewing or establishing standards. Various working groups within these subcommittees focus on the development and updating of specific standards relevant to the digital identity lifecycle, including:
1. ISO/IEC JTC 1/SC 37: Biometrics
2. ISO/IEC JTC 1/SC 27: IT Security Techniques
3. ISO/IEC JTC 1/SC 17: Cards and Personal Identification
4. ISO/IEC JTC 1/SC 6: Telecommunications and information exchange between systems (standards on digital signature/PKI)

There are also technical standards built for identity systems that include: biometrics, image standard biometrics; data interchange format; card/smart card; digital signature; 2D barcode, and federation protocols.

Problems that FIs face today (7)

The evolution of digital channels has resulted in increased remote availability of goods and services, but the corresponding identity verification process has largely been left behind. The failure of identification services to digitize in line with evolving digital channels has led to issues that must be resolved if the promise of an increasingly digital economy is to be realized for customers and FIs.

The need of the hour is an enriched form of digital identification that digital ID provides, an adaptable set of additional required data attributes, and facilitation of the sharing of this enriched ID across a trusted network.

Blockchain: Distributed Ledger Technology (DLT)

What is blockchain? (8)
Digital Identity and Blockchain

A blockchain is a growing list of records, called blocks, which are linked through the use of cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree root hash).

In cryptography and computer science, a hash tree, or Merkle tree, is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes.

By design, a blockchain is resistant to modification of data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."

A blockchain is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without altering all subsequent blocks. This allows participants to verify and audit transactions independently and relatively inexpensively.

*How blockchain works (15)*

*History of blockchain (8)*

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system that would prevent tampering with document timestamps. In 1992, Bayer, Haber, and Stornetta incorporated Merkle trees into the design, and that improved efficiency by allowing several document certificates to be collected into one block.

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to add blocks to the chain without requiring them to be signed by a trusted party (6). The design was implemented the following year by Nakamoto as a core component of the cryptocurrency Bitcoin, where it serves as the public ledger for all transactions on the network.
Digital Identity and Blockchain

Uses and Success Stories of Blockchain (1)

1) Bitcoin and global cryptocurrency

The blockchain industry exists due to the 2008 paper and code that the pseudonymous Satoshi Nakamoto published for a decentralized cryptocurrency network with a unique proof-of-work incentive model. The results: one of the largest distributed computing projects in the world, eight years of operation without a breach of the core blockchain, a community of thousands of developers and start-ups, and a cryptocurrency generating headlines nearly every day.

2) Ethereum: smart contracts and decentralized apps

Ethereum has enjoyed similar success. Originally proposed in late 2013 by Vitalik Buterin to address Bitcoin’s lack of a scripting language, it has grown into a community of more than 30,000 developers and spawned the Enterprise Ethereum Alliance, a global consortium creating a private permissioned version of the public Ethereum network.

Now we need a public blockchain whose purpose is identity for all.

As powerful as the Bitcoin and Ethereum networks are, providing identity for all was never their core purpose. They were not engineered from the ground up for the unique requirements of a global public utility exclusively for decentralized identity. But just as the Bitcoin and Ethereum networks are now frequently used with each other, both could interoperate with a new public blockchain designed for this purpose.

Blockchain standards (10)

The World Wide Web Consortium (W3C; https://www.w3.org) held a workshop in June 2016 to examine aspects of blockchains that relate to Web technologies and identify specific technologies mature enough to be considered for standardization. After issuing a report, it has formed many new groups to address these topics, including the following:

- Credentials Community Group
- Digital Verification Community Group
- Blockchain Community Group
- Verifiable Claims Working Group
- Interledger Community Group

The International Organization for Standardization (ISO; https://www.iso.org/) has also launched a technical committee (TC) 307 on blockchain and distributed ledger technologies with liaisons with several other ISO committees and other relevant standards-developing organizations. The scope of ISO/TC 307 is “Standardisation of blockchain technologies and distributed ledger technologies.”

Apart from the above, there are also communities such as Bitcoin, Linux Foundation, and Openchain Project developing their own standard specifications. The Cloud Standards Customer Council produced a document summarizing existing needs from a business perspective and offering a reference architecture that could be used in further standardization efforts.

Despite initial successful uptake, current blockchain methods have exhibit gaps and limitations in areas related to scalability, flexibility, and governance. Clearly, standardization activity will be required to enable these technologies to be interoperable.

Advantages of Blockchain (9)
Digital Identity and Blockchain

The key benefits of blockchain for financial institutions and business are: greater transparency, enhanced security, improved traceability, increased efficiency and speed of transactions, and reduced costs. Blockchain also alleviates customers’ concerns with respect to their data privacy and protection.

Banks are interested in this technology, because it has the potential to speed up back office settlement systems to increase efficiency and reduce KYC costs.

How Blockchain Can Resolve Digital Identity Issues (1) (2) (3) (11)(15)

The current system of managing identity and validating customers is based on the notion of centralized data, which can be a huge risk, because it is a potential single point of failure. For example, the Equifax breach is a clear example of such a disaster.

The governments of Estonia and India have experimented with centralized digital IDs. An individual’s ID can be used to vote, file taxes, withdraw funds from banks, register property, and comply with other government reporting requirements. Since digital IDs are issued by governments, the information collected is stored in a centralized database. Centralized storage of data creates a single point of failure. To keep such data secure, extremely strict controls and protocols need to be in place (11).

Blockchain is a decentralized root of trust that nobody owns, but everyone can use. Blockchains replace the trust of humans with the trust of mathematics/cryptography. Blockchain works on a consensus algorithm, spanning over many different machines and replicated by many different entities in a decentralized network.

The decentralized nature of blockchain makes it a perfect solution to address digital identity privacy and integrity constraints. Blockchains can ensure that a user’s single digital identity is stored in a secure and incorruptible manner. This single digital identity can always be up-to-date with the latest user information (11).

It will work this way: a customer shares his/her digital identity/KYC documents with a blockchain-enabled FI to authenticate herself and qualify her digital identity on the DLT platform. The institution can then share customers’ data with other entities for legitimate purposes, only after receiving the customer’s consent. This facility benefits all parties in saving time and money by eliminating the need for KYC at multiple places within or outside the country, thereby optimizing costs involved in accurately establishing identities. With a single identity across the globe, it also aids regulators to monitor fraudulent activities, such as money laundering, more effectively.
The advantage of a blockchain-based identity system over traditional ones is its ability to record each identity shared in the global network and maintain continually reconciled data throughout the network. The technology empowers consumers to restrict the sharing of their identities with only trusted local or remote entities (11).

Blockchain can be used to create a platform that protects individuals’ identities from theft and massively reduces fraudulent activities (12). Given this potential, companies are rushing to develop blockchain-powered solutions for digital identity management and authentication. Blockchain-based information-sharing schemes would be the future for digital identity.

Blockchain and Digital Identity Programs In-flight

Successful digital identity programs implemented by countries:

*Aadhaar Identity System India*—*Biometric-Based* (6)

The Unique Identification Authority of India (UIDAI) has issued a unique ID number, known as Aadhaar, to more than 1 billion residents. Photograph, fingerprints, and irises of each resident are captured before issuing an Aadhaar. It is the world’s largest multimodal biometric database, and more than 93 percent of Indians now have a digital identity as a result of this system.

*Smart eID in Pakistan*—*Biometrics and Smart Card* (6)

Pakistan’s National Database and Registration Authority (NADRA) has issued over 121 million ID cards, and hence registered 98 percent of its adult citizens over the age of 18. Over the years, Pakistan’s ID card has evolved into a smart eID that contains multi-biometric features to meet the challenges of a digitally connected world. NADRA is now one of the world’s leading suppliers of eID services. It also designed its cards to meet the needs of its citizens living outside the country. As a result, its smart eID is known as National Identity Card for Overseas Pakistanis (NICOP).

*eID with Digital Certificate in Peru* (6)
Digital Identity and Blockchain

Peru’s National Electronic ID Card (DNie), issued by the National Registry of Identification and Civil Status (RENIEC), was considered to be the best ID card in Latin America during the 2015 High Security Printing Latin American Conference in Lima. RENIEC, an autonomous entity with functions including civil registration, identification, and digital signatures, has issued 30 million eIDs covering almost the entire population of the country. The DNie provides Peruvian citizens with a digital identity, which can be authenticated physically and virtually. The DNie includes two digital certificates, which allow the cardholder to sign electronic documents with the same probative value as a handwritten signature.

ID-Kaart in Estonia—Smart Card and Mobile ID (6)

Estonia has the most highly developed national ID card system in the world (Williams-Grut, 2016). It has issued 1.3 million of its smart ID-Kaarts, each with a unique identifier that allows citizens to access over 1,000 public services, such as health care, online tax filing, and online voting. Estonia is now one of the most digitally advanced nations in the world with regard to public services. It wants to become a “country as a service,” where secure digital identity plays a central role. Key identifying data, such as signatures, are stored in the system alongside a unique number, used by citizens as a unique identifier to sign documents online and verify online identity. The ID-Kaart has advanced electronic functions that facilitate secure authentication and legally binding digital signatures that may be used for nationwide online services. The eID infrastructure is scalable, flexible, interoperable, and standards-based.

The ID-Kaart is a secure credential for accessing public services. To sign a document digitally, a communication model using standardized workflows in the form of a common document format (DigiDoc) has been employed. DigiDoc is based on XML Advanced Electronic Signatures Standard (XAdes), which is a profile of that standard. XAdes defines a format that enables structurally storing data signatures and security attributes associated with digital signatures, and hence caters to common understanding and interoperability.

Blockchain-Based Digital Identity Initiatives by Banks

Consortium of Spanish banks moving ahead with blockchain-based digital identity platform (12)

Supported by eight companies (Abanca, Bankia, Caixabank, Caixa Ontinyent, Ibercaja, Kutxabank, Liberbank, and Unicaja Bank), and led by Cecabank in collaboration with Grant Thornton, the Niuron Consortium was established in 2017 with the aim of building tools designed to combat money laundering and boost KYC efforts.

Five members of the coalition kicked off a project to verify the identities of new clients and share the data with other consortium members. The project is the continuation of a proof of concept stage completed in September 2017 that demonstrated improvements in cybersecurity and the traceability of operations, increased transparency and privacy, savings in costs due to removing intermediaries, and ultimately made the client the owner of its data.

BBVA is also using blockchain-based platforms for closing revolving long-term credit lines and corporate and syndicated loans.

Canadian banks’ identity-sharing ecosystems where the banks are relevant (13)
Digital Identity and Blockchain

In Canada, the financial institutions recognized that it was important to be relevant in customer authentication and ID validation. They recognized that it is essential that they deliver user experiences that re-intermediate them in their customer’s lives.

They began in partnership with SecureKey Technologies by initially launching the SecureKey ConciergeTM service, allowing citizens to authenticate a variety of high-value secure services utilizing their trusted bank credentials. Over 7 million credentials have now been registered in the service, and hundreds of thousands are added per month. The service receives accolades for its privacy stance, in that the bank never knows the service a user is accessing, and the government never knows the credential provider.

Royal Bank, TD Bank, Scotia Bank, CIBC, Bank of Montreal, and Desjardins invested CAD$27 million into SecureKey to accelerate the journey and help develop a true identity and attribute-sharing ecosystem where the banks were relevant. The new service enables attribute-sharing and consumption to and from other parties as well (e.g., Telco and government), but it is the bank that is central in both creating the digital enablement and managing the nodes of the network. Each of the banks placed a senior executive on the SecureKey steering committee to manage governance and prioritization.

The banks felt strongly that while they needed to differentiate their own offerings, it was essential to work together in the development of a national standard, whereby the bank becomes relevant by providing value to customers in every experience—from renting an apartment, to opening a Telco account, to accessing health and government services. Monetization of data was clearly a driver, but removing friction for customer onboarding with third-party services, reducing risk for companies (with cross-validation of attributes), and being present to improve the customer experience (with IDV, payment initiation, lending)—and doing all of this now before PSD2 regulation allows others to lead—were the main factors in banks deciding to move ahead with SecureKey.

Advantages for Banks in Being Part of a Blockchain Digital Identity Network

Banks have built trust with their customers and organizations. Many banks have a wide geographical presence. Based on these key advantages, banks can benefit by investing in a blockchain network for client identification. This is highly relevant, because all credit organizations must perform KYC when processing applications. Blockchain enables users to be identified on a single occasion by a trusted bank, and this information is stored securely with access granted to other banks in the system (14).

Once the bank establishes such a blockchain network for client identification, the opportunities are endless, whereby the technology can be extended for:

- reducing costs and making faster bank-to-bank and international transfers
- looking at possible alternatives to the SWIFT bank transfer system
- opening accounts and financing
- managing documents, etc.

The blockchain technology will provide banks with efficiency, speed, security, and reduced costs in many of their processes. This will directly result in both a price reduction and improvement in the quality of services for end-users.

The benefits for FI are illustrated in the following diagram (3):
Opportunities for Banks in This Space

In 2016, the World Economic Forum recognized that identity is central to the financial services industry, enabling delivery of core financial products and services.

Each percentage of digital onboarding is estimated to be worth about $100m, which makes a clear business case for the banks to adopt.

Identity also opens new markets. As of 2014, 2 billion individuals, primarily in emerging markets, were cut off from financial services, in part because they lacked identification or didn’t have bank accounts.

Digital identity has great potential to improve core financial service processes and products.

Apart from monetization of data, banks have opportunities to re-intermediate in their customers’ lives by becoming relevant in:

- Renting an apartment
- Opening a Telco account
- Accessing health services and government services, etc.

Challenges for Banks in Adopting Blockchain

While there are clear benefits and advantages, FIs still face the following challenges while adopting blockchain:

- Handling the complexity and open-source nature of blockchain technology
- Taking technical jargon to customers
- Environmental sustainability issues due to the high amount of machine/electricity needs
Digital Identity and Blockchain

- Lack of standards for blockchain implementations
- Issues of data-sharing across other FIs and service providers
- The stringent rules and regulations around BSA and privacy
- Putting in place a framework of effective and efficient control and monitoring structure given highly technical nature
- The need to validate new technology and provide confidence to internal audit, compliance, and risk teams
- There is still a lot of work to do before the major regulatory hurdles to blockchain adoption are cleared
- Before deploying blockchain applications at scale, FIs will have to learn to navigate a new world of digital risk. One little-talked-about but critical factor in blockchain’s widespread adoption is governance—and bridging the gap among innovators, technologists, regulators, business leaders, and governance teams remains a challenge. Enterprises need a comprehensive controls framework for blockchain to ensure their deployments will meet governance, risk management, and controls requirements (15).

Impact of Blockchain on Audit and Assurance Process

Blockchain has rapidly grown, and a number of R&D and implementation efforts are in progress. As with any new technology blockchain, there are also trust implications for risk and governance professionals.

Issues revolve around the fact that blockchain was never designed with an audit trail or control environment in mind—it was built as a pure technology solution. Enterprises must build in governance if they want to validate blockchain applications from an audit perspective. There is a common misperception that immutability of the blockchain means there is no need for governance or internal audit. This is not true. The blockchain itself may be sound, but the entire workflow that runs on top of the blockchain still requires governance and validation, just like any other business process. There are several variants of blockchain technology organizations can chose to enable a specific use case that will dictate the platform, protocol, consensus, and encryption mechanisms; each has a distinct set of risks.

Traditional audit approaches don’t work with blockchain, as we cannot perform a point-in-time, retrospective, sample-based analysis. Applying traditional audit approaches to blockchain applications requires an exponential increase of both resources and time, simply because it is tedious to go through a distributed chain. The exponential volume makes the traditional sample-based analysis ineffective.

From a risk perspective, there is no framework development for evaluating blockchain risk. Lack of knowledge creates skill gap and makes people believe it is almost impossible to audit blockchains.

The following are the new opportunities and challenges that blockchain brings to the audit and assurance process:

- Possibility of automated audits: The automation of verification process will drive cost efficiencies in the audit environment.
- Testing of whole population rather than substantive sample check due to inherent nature of blockchain technology.
- Vulnerability of software on which blockchain is implemented: This will need audit to check the operational effectiveness of internal IT controls.
- The following are key challenges:
Digital Identity and Blockchain

- Blockchain is a relatively new technology. Audit teams may not yet have the expertise or guidance to know how to fully gain comfort with a system that puts trust in advanced cryptographic algorithms; there is a longer learning curve.
- The controls will have to be different due to the distributed nature: auditors need to ask difficult questions. Who controls the blockchain? Who gets access? Where are the servers, and what physical and digital controls exist? Who monitors activity? Is the technology in fact doing what it claims to do?
- Technical expertise is not easily available: in the 2017 Global Digital IQ Survey, some 86 percent of financial services executives said that their organizations haven’t yet developed necessary blockchain skills. Few companies have internal audit teams with enough expertise to provide any sort of assurance around the blockchain technology and the associated work. Most internal audit teams are always looking for technical expertise, but finding these resources can be tough.

Despite the high potential, there are still risks associated with blockchain. How do we get assurance that the information is accurate?

When we think of audit, compliance, or regulatory activity, it is all about standardization. However, blockchain is a form of computer science with very little standardization. For example, different clients can use different types of software and architecture. To tackle this, a different professional audit mindset and additional expertise will be required.

Firms such as PwC are already working on risk frameworks for auditing blockchain implementations.

Conclusion

Financial institutions as early adopters of this technology can reap the various benefits that a blockchain digital identity ecosystem can bring forth.

The regulators will, and should, regulate products. However, blockchain is a technology at present and expecting to regulate it is the same as expecting them to regulate relational databases. “It is difficult” is an understatement. The regulators should embrace the potential opportunities and utilize the rules they currently have in place for banking and financial services, but adjust, revise, or create new rules to mitigate the risks of blockchain technology (15).

Meanwhile, there is an urgent need for creating the audit frameworks, processes, and skills required to support such implementations.

Auditors will need to raise the bar by providing increasingly complex assurance services in more agile business environments and in support of digital transformation.
Digital Identity and Blockchain

References
17. https://towardsdatascience.com/https-medium-com-shaanray-how-blockchains-will-solve-privacy-88944f3c67f0