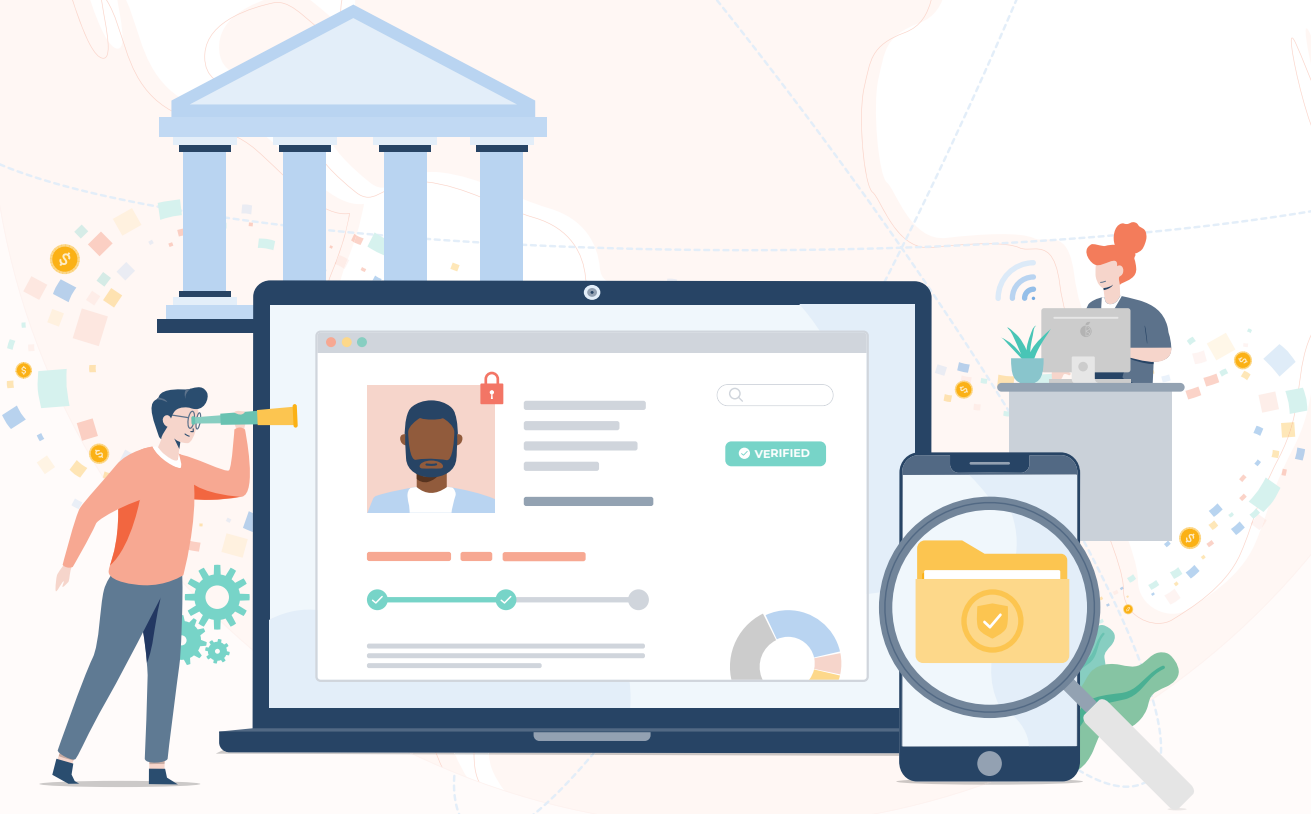
LIQUIDUS

Banking on the Chain

The golden ticket to technological transformation for the financial services industry



Contents

Executive summary

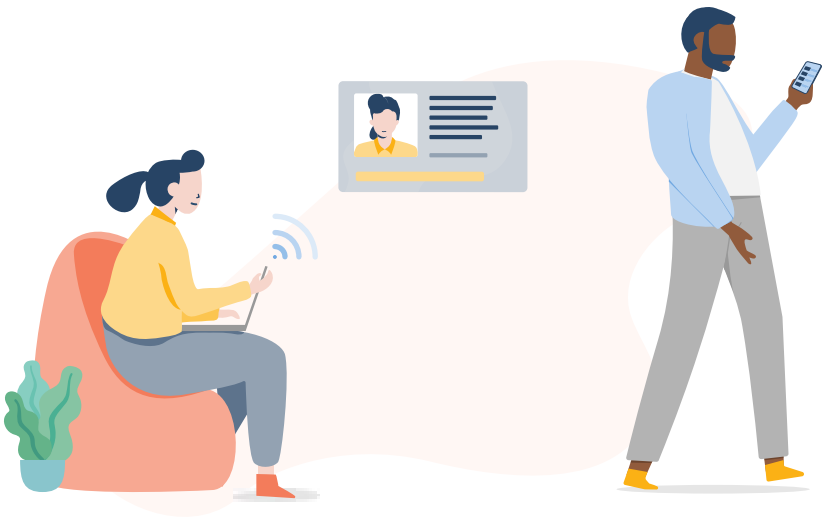
Transitioning into a future-ready digital financial institution involves a deep strategy for customer and employee digital identities. Digital infrastructure designed around compliant identities removes barriers for onboarding clients, and reduces the costs related to most financial transactions

Digital customer identity is essential, as regulators such as the Financial Action Task Force (FATF) have designed regulation around digital wallets and asset ownership. They have stated how it is key to have strong digital identities on both sides of a transaction for AML, KYC, and counter terrorism legislation.

Many financial institutions around the world are looking towards blockchain as an infrastructure to build the foundations of a future-ready financial institution. While not necessarily essential, blockchain brings with it:

- Built-in disaster recovery/failover
- Built-in security/immutability (zero-trust paradigm)
- Ready for the distributed enterprise (SaaS etc.)
- Ready access for financial regulators and third party auditors: evidence-based ledger compliance
- Heightened opportunities within the digital asset markets such as digital asset custody, trading and instant settling.

This report provides a look into the opportunities and challenges that blockchain can bring to financial institutions and highlights some key facts and statistics about what's happening today.



Introduction

When the Covid-19 pandemic began sweeping the world in March 2020, the digital economy stepped to center stage. Without warning, but also without many alternatives, businesses and individuals dove into a world of physical distancing by moving whatever activity they could to the internet. Outdated, analogue business models were replaced practically overnight with digital processes. Businesses that could not adapt quickly lost revenue. In order to facilitate this massive and sudden shift to online marketplaces,many governments loosened regulation surrounding occupational licensing and technology.

While the "crypto movement" has been a phenomenon unfolding for over a decade, COVID-19 provided both a nesessary push and a huge opportunity for blockchain technology.

Deregulation, however, can bring its own set of problems. A major challenge in this increasingly digital world is the need for data to be accessed quickly and easily, yet securely. Every day, millions of transactions are occurring, each one leaving a trail of essential data that firms and individuals must be able to access efficiently and reference in a compliant manner. At the same time, this data is a gold mine for fraudulent actors, and data breaches and security threats have peppered the news. It is difficult for financial institutions to balance the need for security with the various international regulations that exist. But is it possible a technological solution to the problem of security and regulation may already exist?

While it has been quietly simmering in the background for some time, it is now quickly moving into the digital banking mainstream.

Blockchain and financial institutions

Blockchain technology is a "secure by design" method for operating digital transactions within a global, consensus-based digital ledger. By the nature of how transactions are recorded within chronological batches (i.e. blocks), each transaction verifies the soundness of all transactions that came before it. This is made possible by digital signatures confirming cryptographic proofs, verified through an incentivized network of servers. This eliminates a great deal of human error from ledger reconciliation via software automation.

Anyone attempting to fraudulently change an entry or otherwise break the integrity of the chain of transactions would be faced with an impossibly expensive task, due to how many copies of the ledger exist. In order to falsify an entry a hacker would need to control more than half of the copies and surpass the associated collective computational power of their paid maintainers. The design of blockchain is data-based, rather than currency-based, and relies on a "common law of the platform" for security through "rules without rulers", or otherwise known as on-chain governance.

Spotlight on blockchain in mainstream markets

Blockchain by its nature reduces friction, increases security, enables transparency, and creates opportunities to reduce cost and enable new revenue streams. Therefore, even though blockchain was created and first adopted in the alternative finance world, it quickly caught the attention of more mainstream enterprises.

Since corporations process transactions that prove ownership and obligation, blockchain can serve as a back-office brainstem for corporate contracts and ledgers that can no longer be fabricated, lost, or stolen. This is disruption-level technology for economic and public policy that could greatly reduce the costs associated with regulation compliance. Globally, financial institutions are taking notice:

- In 2016, the European Payments Council reported 90% of their members expected blockchain to change how firms did business in less than 10 years, and they have taken steps to prepare for this change.
- Over 200 banks worldwide are working on or have begun using blockchain.
- Nearly half of the 26 public banks in China have deployed blockchain in some form for a variety of uses, according to CEBNet.

Additionally, a study by McKinsey found that origination and sales produce 65% of bank profits worldwide, equal to about $115 trillion in 2016. Thus, improving the ability to bring on (and to bring on (and keep) more customers from more demographics, especially financially underserved populations, is essential to retaining market share. With increasing competition from challenger banks and rising customer acquisition costs, financial institutions need to reduce the cost of on-boarding new customers and the general overhead throughout a customer lifecycle. Blockchain and open banking can free up resources and increase profitability, while banks that provide frictionless, digital first account opening processes are more likely to gain the business of younger consumers.

90%

Of EPC members expect blockchain to change how they do business in less than 10 years - *2016 EPC Report*

Early adopters find an advantage

Cross border payments are typically costly and time consuming. Transactions that take place between distant regions of the world can involve multiple banks corresponding to settle balances involving foreign exchange.

More recent developments in the banking world have started paving the way for blockchain technologies to ease this problem. In 2018, the Global Financial Innovation Network (GFiN) formed, ballooning to over 43 financial system regulators, and in 2019 they spent a year piloting a system for cross-border transactions.

International cooperation on a large scale has been modeled by the Monetary Authority of Singapore (MAS). The MAS has signed 33 FinTech Cooperation Agreements with regulatory counterparts around the world since 2016. These contracts formalize agreements for sharing information such as blacklists, provide cross-sell referrals, and cooperate on other innovative projects stimulating the flow of commerce with reduced friction.

One of these agreements between the MAS and the Hong Kong Monetary Authority (HKMA) encourages information sharing between jurisdictions by granting referrals in one jurisdiction to FinTechs that meet all regulatory requirements in the other jurisdictions. Since some institutions work in both jurisdictions, this can facilitate consistency in best practices among the branches of that institution, as well as create significant synergy between multiple institutions.

$4 billion

Approximate annual savings for institutions in cross-border payments using blockchain technology. - *2019 McKinsey Report*

Using blockchain rails to securely and efficiently facilitate interjurisdictional gross-settlement payments is a boon for both banks and their clients. In fact, McKinsey reports that institutions could save approximately $4 billion annually in cross-border payments using blockchain technology, if only by preventing identity fraud in those transactions.

Identity fraud prevention

Identity theft and cybercrime cost individuals and companies billions of dollars each year. As an example, 21% of adults in the UK have had to cancel or replace credit and debit cards in the last year due to attempted fraud, according to research by comparethemarket.com. Additionally, research by Javelin indicates that banks worldwide may lose between $15-20 billion from identity fraud in a single year.

Blockchain technology presents an opportunity to revolutionise the credential sector by offering a more effective, scalable, and secure platform for the production and use of credentials. Malta and The Bahamas have been using Blockcerts (on the Ethereum blockchain) to notariseeducation credentials since 2017. The more complex and developed the economy, the more it depends on efficient and effective credential infrastructure and production.

Blockchain-based identity is an effective and cost-effective paradigm for fraud prevention. In particular, all of the verifications baked into the system provide real-time guardrails for both the authenticity and authority of whomever is involved in any digital transaction.All relevant contextual and historical information is available as needed for verification.

Blockchain-based identity is an effective and cost-effective paradigm for fraud prevention. In particular, all of the verifications baked into the system provide real-time guardrails for both the authenticity and authority of whomever is involved in any digital transaction.

Such digital identities or identifiers become certified credentials that are completely portable and user-owned. Therefore, they can travel with a client wherever they happen to interact with a regulated entity. From a financial institution's perspective, a credential is a bundle of:

- Identity (the customer)
- Registry (what compliance details do we know about them?)
- Assessment and evaluation (how have the compliance details been verified, and by whom, with what authority)
- Storage, maintenance and recall (access to, and confidence in the validity of the above)

To highlight the security of blockchain-based, identity-enabled transactions, the: vendor, payment itself, identity of the buyer, and bank account from which the payment is being pulled are all verified.

This rich, perpetual visibility into customer activity ensures that if something is suspicious at any point in the transaction history with anyone involved, the in-flight transaction can be flagged and accounts may be frozen temporarily and reported as necessary.

Let your clients control their data

The granularity of consent with which identity access may be controlled is also a major selling point for customers, eliminating the redundancy of having to share the same documents and information with each new service provider, all while improving auditability for all parties involved.

Oversharing of data when it is not needed can become a thing of the past, and not only would this be a major improvement in operational excellence, but it is something customers have been demanding

Simon-Kucher and Partners reported in 2019 that nearly 75% of bank customers are unlikely to give consent for their banks to share their personal and financial data with third parties. Since credit risk is tightly coupled with identity fraud, streamlining the process of identity verification helps to inform costs and constraints around credit-allocation with better information about customers. Customers who receive personalized product recommendations with bespoke prices for their credit are more likely to stay with the organization.

90%

Cost savings by institutions when using digital identification to onboard new customers - *2019 McKinsey Report*

There are inevitably times when a person's identity and documentation must be verified in person and/or with documentation, such as a passport. However, this may be completed once and reused as a cryptographically secured proof of identity with any service provider who would recognize the proof. In the blockchain paradigm, this flow of information is directly between the service provider and the customer, though signed attestations of it are propagated throughout the network for verification purposes.

In this way, documents no longer need to be scanned or photocopied and sent to others in ways that can be intercepted. Meanwhile, various third-party providers and identity brokers may provide further proofs on top (i.e. attestations), serving to strengthen the ecosystem's overall confidence in the veracity of an identity, its linked documents, and all associated metadata. Attestations express identity as a form of property rights. Yet unlike rights over most forms of property, others could potentially add to your identity without your involvement, knowledge, or even consent.

5 days to 1 hour

Time reduced to onboard a customer due to increase in technology spend - *Saxo Bank*

This seamless, automated experience benefits banks by providing the most up to date and relevant information to employees working with new customers, with far less manual processing and delays. For example:

- McKinsey reported in 2019 that using digital identification could save institutions that use it up to 90 percent of the cost associated with the time it takes to onboard new customers and verify their identities.
- By increasing its technology spending by 40 percent, Danish investment bank Saxo has reduced the onboarding process for a "non-complex customer" from five days to less than an hour. In April 2020, they onboarded a record 18,000 customers, up from the relatively static monthly average of 1,500.

National initiatives for electronic identification

With electronic signatures becoming more commonplace, having the ability to digitally verify who is signing is absolutely necessary in order to avoid fraud. Digital identity systems, then, need to be developed with appropriate security and oversight. According to the FATF Q4 guidance draft, authorities need to work together to "develop clear guidelines or regulations allowing the appropriate, risk-based use of reliable, independent digital ID systems by entities regulated for AML/CFT purposes."

The United Kingdom went public with their Gov.UK Verify digital identity in 2016, though the project is currently only used for a few different government-related activities. This limited use likely caused relatively slow initial adoption that nonetheless increased tremendously when the Covid pandemic caused more people to apply for Universal Credit.

In the summer of 2017 Zug, Switzerland (aka Crypto Valley) set out to create the world's first live implementation of a self-sovereign government-issued identity project on the Ethereum blockchain. Catalonia's IdentiCAT was launched in Q3 2019 by the Department for Digital Policies and Administration with the intention to give citizens "exclusive ownership" and management of their own digital identities. In addition, the digital identity has a legal guarantee that it is in compliance with data protection laws and can be used in both public (government) and private transactions.

Reduce compliance cost

Digital identity creates an incredible opportunity to cut costs for financial institutions. In addition to the costs associated with identity theft, there are significant costs associated with keeping in compliance to prevent identity fraud. Global Anti-Money Laundering (AML) efforts cost over $8 billion in 2017, as reported by WealthInsight, an increase of 36% over four years previous.

Using blockchain in KYC processes could save between $160 million and $420 million annually, allowing banks to reduce the number of employees manually processing these requests by 10-30%.

It is more effective and less costly to identify fraud in its earliest stages. Doing so requires constant vigilance, but without automated solutions this requires continually poring over reports,spreadsheets and making phone calls. A Thomson Reuters Survey from 2016 reported that AML checks and Customer Due Diligence (CDD) cost banks, on average, about $58 million a year, and some up to roughly $435 million a year.

Due diligence takes time and effort and tends to focus on origination. For example, once a customer is onboarded and the KYC is complete, there is often little to no follow-up to see if the client's risk profile has changed. Sometimes it's a paper file containing the client information that is stored in a cabinet, away from databases and double-checks that could catch a red flag.

KYC can delay transactions for as long as fifty days. The cost of compliance, including regulatory fines, for AML was estimated to be around $10 billion globally in 2014. The average cost of compliance is $950K for every $1 billion under management.

Blockchain technology presents possible solutions to reduce the cost of compliance. According to a Goldman Sachs Report, Case Study 7, using blockchain in KYC processes could save between $160 million and $420 million annually, allowing banks to reduce the number of employees manually processing these requests by 10-30%. It would also reduce HR costs associated with these employees. Aside from the overhead saved by reducing staff, operational savings could be approximately $2.5 billion dollars, with higher, more automated compliance reducing AML penalties by $500 million - $2 billion dollars.

Custodial services using digital currencies

Custodial arrangements for securities - holding client assets to keep them secure and to trade them as requested - are an enormous part of the global financial market. More than $114 trillion in assets are held by mostly four major banks. Even though this huge amount was held but mostly four banks, only only $1.6 billion[1] was invested between 2012 and 2020, over 46 deals in companies that offer institutional-focused custody services for cryptocurrencies (and other assets in the future).

The Office of the Comptroller of the Currency (OCC), a federal banking regulator in the U.S., published a public letter in July 2020 announcing its approval for nationally chartered banks to provide custody services for cryptocurrencies.

Digital assets are becoming increasingly important as a piece of a well-diversified portfolio. A 2020 survey by Fidelity Digital assets found that, of 800 institutions around the world, 60% believe digital assets belong in their investment portfolios. Of those, 36% reported already being invested in digital assets; 45% of those were European institutions and only 27% were American.

[1] based on the figures published in the July 2020 report by The Block.

The Office of the Comptroller of the Currency (OCC), a federal banking regulator in the U.S., published a public letter in July 2020 announcing its approval for nationally chartered banks to provide custody services for cryptocurrencies. Meanwhile, the German government is examining digitized shares and issuing digital bonds, replacing securities certification with a crypto custodian for streamlined technical and regulatory purposes.

However, news surrounding security breaches in cryptocurrency exchanges may undermine the public's trust in these assets. These breaches tend to be caused by poor Operations Security (OpSec) practices, or the security of auxiliary systems, rather than insecurity in the blockchain itself. Therefore, if institutions are going to join the digital assets revolution, they will need to step up their OpSec game.

Securities settlement

In 2017, contracts and trades in the United States cleared through the Fixed Income Clearing Corporation (FICC) were worth $1.09 quadrillion, and those cleared through the National Securities Clearing Corporation (NSCC) were worth $240.5 trillion. LCH.Clearnet, a British clearinghouse, did $920 trillion worth of compression volume that same year.

The International Swaps and Derivatives Association (ISDA) reports 70% of transactions currently take at least an hour to reconcile. Of what remains, 15% require more than a day for experts to work with all of the parties involved to resolve any disagreements within the records when the transactions occur. In a select number of single transactions (2%) $1 million to $2 million is lost per transaction.

$10 billion

Amount of annual savings that the largest investment banks would gain by replacing manual reconciliation with blockchain in the clearing and settlement process - *2017 Accenture Report*

In 2017 Accenture estimated that if the largest investment banks would replace the manual reconciliation and communication overhead with blockchain, they could save up to $10 billion annually in the clearing and settlement process. Some very large organizations are doing just that. A 2018 test by the Bank of Canada, TMX Group - the Toronto Stock Exchange operator - and Payments Canada showed that automating instantaneous securities settlements (thereby reducing counterparty risk) becomes possible with blockchain.

Transparency, redundancy and seamless collaboration

Most of the expenses associated with cross border payments, compliance, and securities settlement,stem from excessive layers of indirection and redundancy. This severely constrains the ability to collaborate effectively across institutions. Blockchain can be used to resolve these issues.

Transparency and collaboration are two sides of the same coin. A major reason why all of the processes mentioned above require significant hands-on labor is due to each financial institution, country, and jurisdiction having their own rules, regulations, and processes. When one organization sends information to a partner organization, some of those same processes and checks and balances have to be run again, but with a different set of rules.

The KYC registry estabished by SWIFT is a start, but with only 1,125 member banks out of the 7,000 in its network, there is still a long way to go towards true adoption as an industry standard. International collaboration, including treaties and global courts, is incredibly costly because most laws only work well in (and may only apply to) a single country.

The Office of the Comptroller of the Currency (OCC), a federal banking regulator in the U.S., published a public letter in July 2020 announcing its approval for nationally chartered banks to provide custody services for cryptocurrencies.

If this process could be carried out seamlessly with blockchain, the world economy would begin to be run like one large organization, minus the bureaucracy. Regulators from any nation could examine documents from, and work with, any financial services unit on the blockchain network and understand the records.

Transaction data is rarely standardized across organizations and sometimes does not contain complete data. With SWIFT MX, ISO 20022 and similar initiatives, data standardization is improving, but it can be difficult to determine the purpose of transactions. Even some processes designed to flag suspicious behavior cause many false positives and important documents, like invoices and clearances, are lost in transmission.

Real-time reconciliation of records across institutions removes the need for a process to eliminate errors that tends to cause errors. Record sharing among a greater number of stakeholders and institutions consequently leads to more transparency. Transparency leads to trust as clients are more inclined to trust an institution when they know all of the other institutions are watching and looking over its shoulder.

A beneficial side effect of a multitude of stakeholders with copies and access to pertinent records is the security found in this redundancy. In case of natural disasters, network crashes or hardware failures, recovering data is as simple as accessing another copy of the blockchain at another institution. The relevant records are shared continually with the guarantee that they cannot be changed or corrupted. Realizing this benefit, most nations in the Carribean region have been actively developing digital asset legislation to attract providers globally to its shores, in order to realize the first Central Bank Digital Currencies.

Challenges with building your own blockchain

While blockchain may seem like a silver bullet for the financial world, building these technologies brings a complex set of hurdles. The technology itself can be difficult to understand and requires skilled technical professionals for implementation. Financial services focused blockchain platforms however, aim to create a seamless onboarding experience with all relevant compliance and data privacy features built in.

Creating a shared banking ecosystem may prove to be quite costly upfront. Internal institutional data structures would need to change in order to communicate efficiently and consistently with other institutions. Agreed upon industry standards, which would first have to be created and decided upon, would need to be communicated and enforced when using the network structure.

Short-term costs of building the blockchain network may be outweighed by the opportunity to boost revenue in other ways by participating in a blockchain ecosystem. Once the system is up and running, it is highly likely that the expenses would be borne among all of the participants, cutting costs in the long term.

The standardization of shared data in digital ledgers has tremendous opportunity to prevent data loss, fraud, and non-compliance. If the hard work of creating consensus for regulations, data standards, and workflow can occur, it will no longer be necessary to check then re-check the compliance of third-party providers.

The challenge of reaching consensus among multiple financial institutions on what data is shared is a huge undertaking. International consensus will need to be established regarding requirements for identity verification. Determining what constitutes acceptable documentation in digital identities for cross-border verification requires unprecedented communication. This is being addressed by global organizations such as the FATF, it will be interesting to see if regulators and quasi-government organizations release any type of governance smart contract to enforce governance and assist in international consensus.

Individual bank systems also face the question of how to reconcile the data they need for legacy systems with the data required for the shared blockchain ecosystem. There is a vast amount of data that is more qualitative - i.e. more informative than statistical - that takes a less structured place within databases and bank processes. Some of it may be specific to a single institution and does not need to be shared with the ecosystem. Banks will need to determine how useful such data truly is in the absence of standard benchmarks, and whether the costs of aggregating the data in a new way the data outweigh the benefit.

The personnel ramifications of these types of adaptations should not be taken lightly. Workflow has often been dictated by the software systems already in place and the "how-we've-always-done-it" mentality, but financial leaders and managers will need to be flexible to determine how workflow needs to change. Legacy systems may still be necessary, but processes should be created based on what works best and most efficiently, and such structural changes are never easy.

Digital assets/utility tokens themselves are very new, and would require significant education for both the professionals and the consumers. They are neither currency nor equity and a lack of regulation surrounding how they work would need to be corrected.

In spite of the challenges, the standardization of shared data in digital ledgers has tremendous opportunity to prevent data loss, fraud, and non-compliance. If the hard work of creating consensus for regulations, data standards, and workflow can occur, it will no longer be necessary to check then re-check the compliance of third-party providers.

Blockchain opportunities, and why not to get left behind

Blockchain technologies provide significant opportunity to streamline processes.

- The distributed ledger model can ease friction in cross-border payments and security settlements.
- Digital identity verification has the ability to create single identity records that can be shared among stakeholders, cannot be falsified, and reduce the vast costs associated with both identity fraud and compliance.
- Custodial accounts using digital currencies provide an opportunity to increase revenue.
- The transparency required to use these types of ecosystems provides security by having multiple copies of the data in multiple places. It also facilitates collaboration because all users have access to the same sets of data.

Nations around the world are experimenting with these technologies to provide further services to their citizens while reducing costs associated with current processes.

Financial institutions could build smart contracts into employee and customer digital IDs. These could be designed to reduce costs for onboarding and compliance of new customers as well as for HR reasons such as when contracts or documents need to be updated.

In addition to all of the advantages this new technology could provide, those who adopt it will likely find new revenue streams and yet unforeseen possibilities for providing value.

One such opportunity is in the form of smart contracts. These contracts can be programmed in the distributed ledger to carry out specific sets of instructions when certain conditions are met. Observational mechanisms, known as oracles, take note of when events occur - e.g. authorized digital signatures are in place, or verified identity reaches a certain age. These conditions then trigger automated follow-up actions, such as sending information to a third party, causing a 401(k) plan rollover, or transferring an IRA.

Today, smart contracts primarily run as part of the larger schema of decentralized finance (DeFi). Given that annualized interest rates in DeFi can be anywhere from 2.5% to 14%, and up to 50% in some market conditions, these kinds of returns are clearly appealing. If banks coordinate with these DeFi initiatives, or even build their own, they would provide their customers seeking high-risk, high-return investments a way to participate in a compliant manner.

Fixed income has been difficult to access for individual investors, preventing access to products that have a risk profile and return that contributes to a well-diversified portfolio. A platform for the syndication of corporate loans can be effectively enabled through smart contracts governing the creation of tradable digital notes, also known as “security tokens.”

Financial institutions could also build smart contracts into employee and customer digital IDs. These could be designed to reduce costs for onboarding and compliance of new customers as well as for HR reasons such as when contracts or documents need to be updated. The possibilities are nearly limitless, but could be tailored to address any repetitive time or cost-intensive activities.

Conclusion

Smart contracts are just one of multiple possibilities that may be developed with automated secure technologies. Not adopting blockchain technologies for the banking industry will result in massive opportunity cost.

Organizations that take advantage of the automation, the cost reduction, and the security while others stick with the status quo, will thrive in the digital economy.

Verified digital identities smooth the challenges currently experienced when attempting to make payments or transfers. There is no need to manually verify each link in the payment chain. Transactions between currencies, countries, and entities can happen more seamlessly. The easier it is for customers, the more they will want to use it, adding new customers to the banking system, building trust, and keeping banks relevant.

Providing on-demand reporting with real-time, automatically audited metrics, blockchain solutions can eliminate the information asymmetries between bank management and the bank's other stake-holders, perhaps most importantly its customers.

Organizations that take advantage of the automation, the cost reduction, and the security while others stick with the status quo, will thrive in the digital economy.

Building a blockchain based infrastructure for a financial institution is a task that can take many years to fully transition. Each financial institution will face different transformational barriers, however institutions will be rewarded with new areas for revenue as well as cost reduction in operations. An important factor around digital transformation into a blockchain based infrastructure is change management both internally and externally. Blockchain offers a variety of advantages for both customers and financial institutions themselves, however, the technology needs to be as simple to use as before, and wherever a new process is in place, full training and education needs to be provided.

The starting point for a digital transformation is a master digital identity, which enables digital onboarding and management of clients from a compliance standpoint. With a verified digital representation of your client, it is then possible for the financial institution to establish the largest area of opportunity depending on the markets they are most prevalent in.

Connect with Liquidus for a free consultation and demonstration of our compliant onboarding software.

For more info please visit:

www.liquidus.io