R3 Reports

If at First You Don't Succeed, Try a Decentralized KYC Platform:

Will Blockchain Technology Give Corporate KYC a Second Chance?

Kevin Rutter

Contents

R3 Research delivers leading insight into the enterprise blockchain industry, from specific real-world application to cross-functional analysis. Drawing from a global team with extensive industry experience, R3 reports stand at the forefront of blockchain research.

If at First you Don't Succeed, Try a Decentralized KYC Platform:

Will Blockchain Technology Give Corporate KYC a Second Chance?

Kevin Rutter*

July 22, 2018

Abstract

In 2014 and 2015 several centralized Know Your Customer (KYC) utilities aimed to address problems with corporate KYC for both banks and their customers. These utilities have had mixed success. While they solved some problems, they also introduced new ones. Blockchain technology enables decentralized KYC platforms, which are a new approach. With the correct architecture, these decentralized platforms can maintain direct customer-bank relationships and avoid the pitfalls from centralizing parts of the corporate KYC process. This paper reviews a self-sovereign approach and a bank-sharing approach. Within most jurisdictions, the self-sovereign approach is the most likely to succeed. Further, the paper addresses the advantages, common issues, and disadvantages a decentralized platform offers relative to centralized utilities. Lastly, it suggests that commercial banks coordinate to pursue a decentralized corporate KYC platform.

1 The Road Towards Corporate KYC Utilities

1.1 Introduction to KYC

Through a process known as Know Your Customer (KYC), commercial banks validate their customers' identities, maintain up-to-date records on their profiles, monitor transactions and habits, and use their ability to report any suspicious activity. The KYC process is essential to client onboarding, screening against sanctions, and addressing an increasing number of financial regulations related to Anti-Money Laundering (AML). Banks also conduct due diligence to protect themselves against fraud and determine whether they should provide or deny particular services for a customer. Table 1 contains a fifty-field example subsection of KYC policy data requirements across seven categories for a high risk corporate customer.

The KYC process involves sourcing, proofing, maintenance, and access management. *Sourcing* is considered the creation of new identities in a commercial bank's record, requiring sufficient information to ensure that a unique and verifiable identity exists. *Proofing* establishes the reliability of the sourced information, often through independent verification with a third party. *Maintenance* involves ensuring that the customer information remains accurate over time. *Access management* involves making sure that customers have access to the right resources, and involves authentication, authorization, and privileging (King et. al, 2016).

*Thank you to Matthew Bradbury, Jane Kenyon, Abbas Ali, Alisa DiCaprio, George Calle, and Gabriella Zak for help and comments.

Table 1: Examples of KYC Data Requirements

Legal Formation	**Entity ID, Legal Name**
Corporate Registration	Registration Authority, Country of Entity's Registration, Date of Corporate Formation, Government Issued ID, Proof of Government ID, Certificate of Incorporation, Memorandum & Articles of Association
Legal Hierarchy	Type, Parent Entity ID, Parent Legal Name, Parent Country of Incorporation, Parent's Registered Address, Parent's Country of Residence, Name of Listed Exchange
Countries of Business	High Risk Countries That Entity Does Business in, % of Entity Revenue Generated in the High Risk Country That Entity Does Business in, Number of Employees
Financial Information	Reporting Currency of financial statement, Total Revenue, Total Asset Size, Total Shareholder's Equity, Name of Auditor, Annual Report
Key Controllers and Directors	Type, Corporate Entity's Full Legal Name, Corporate: ID/MEI, List of Shareholders
Beneficial Ownership Reporting	Type of Beneficial Owner, Level of Beneficial Owner, % ownership of KYC Entity, Position, First Name, Last Name, Date of Birth, Address, Country of Residence, Passport, Corporate Legal Name, Entity Booking Jurisdiction, Company Type

Source: R3

1.2 How KYC is Broken

The current corporate KYC system is inefficient for both customers and commercial banks. First, different banks ask for the same information, causing redundant effort for customers and for financial institutions performing similar data collection. A corporate might have to submit information to 15-20 banks. If one bank has separate legal entities, there can be separate onboarding processes within the same bank.

Second, each bank requires diverse additional types of information, introducing more complexity for customers. Banks in different jurisdictions ask for different types of information in different forms. Even banks in the same jurisdiction will request different information for their data collection processes.

Third, due to poor customer-bank communication, banks are often unable to process the appropriate data on behalf of the customers in a timely manner. This is largely because the current method for gathering and maintaining data introduces difficulties and inaccuracies for both banks and customers. Many identity documents remain paper-based, and submitting these documents is often an error-prone and manual process through email, mail, or even fax. Exceptions must be thoroughly documented, and many times banks ask for additional information from the clients. Often, third-party vendors can verify information accuracy, but accreditations along existing channels add delays. Further, banks have difficulties managing client data given internal complications aligning and sharing information across departments at commercial banks.

1.3 The Effects of These Problems

Due to these problems, KYC is often problematic for customers, involving lengthy onboarding times. Once documentation has arrived at a commercial bank, onboarding can still take between 2-4 months. These delays mean that customers cannot quickly access their desired financial services. Slow onboarding is detrimental to banks as well, as delays hurt their profitability. Particularly poor customer service at one bank may lead to customers pursuing other banking relationships.

KYC is also an expensive operating cost for the banks. Of the world's top financial firms, 10%

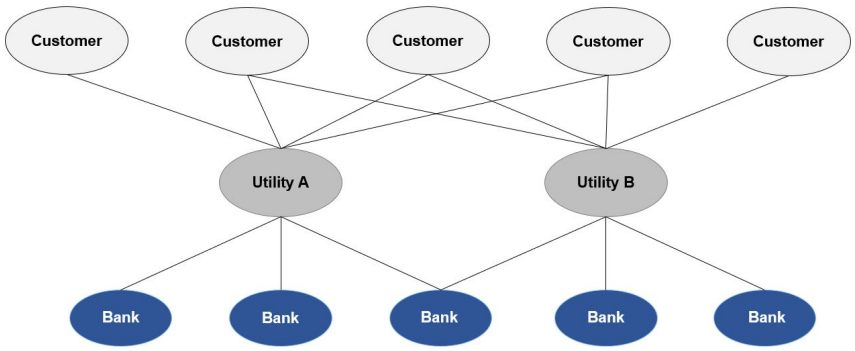
are spending over $100 million annually each on KYC, and some are spending up to $500 million (Thomson Reuters, 2017). Much of the cost is due to process inefficiency and redundancy, and the cost of compliance continues to rise industry-wide.

Additionally, the limitations of the current KYC approach magnify regulatory challenges. Banks receive staggering regulatory fines when there are compliance failures. For example, in 2014 a bank paid a $8.9 billion penalty due to sanctions violations. The size of these fines contribute to a risk-averse culture and hesitance to innovate, even though increasing regulatory pressures require financial institutions to enhance their on-boarding processes. When there is an inquiry, the current disparate state of records makes responding difficult — such as the delays faced when banks struggled to respond to a request by the FCA in the United Kingdom in a timely fashion in the wake of the Panama Papers.

1.4 Centralized Utilities of 2014-2015

KYC is rarely a competitive advantage for a bank. A bank may have some advantages over competitors for certain parts of their KYC processes, but in general, KYC is a non-differentiating service. Therefore, the banks recognized the opportunity to mutualize costs and form a new type of infrastructure streamlining the process.

Figure 1: Centralized KYC Utility



Source: Celent, Oliver Wyman

In 2014 and 2015, the KYC utility industry launched with four major players emerging as leaders within the market: SWIFT, Depository Trust & Clearing Corporation (DTCC), Markit-Genpact, and Thomson Reuters. Thomson Reuters eventually purchased the DTCC solution, Clarient. Despite overlap amongst the platforms in client offering and target market, they include key defining characteristics that exist across implementations. See Table 2 for more information on these three solutions.

These utilities have experienced some success, but certain shortcomings have limited their adoption. A 2018 International Chamber of Commerce Survey stated that despite the challenges of due diligence and KYC, 34% of respondents said they do not use a KYC utility service of any form, largely due to cost, operational considerations, and the challenge of complex technical integration. Some of these issues have led to growing support across banks to explore decentralized approaches to KYC utilities leveraging blockchain technology.

2 Decentralized KYC Platforms

2.1 What is a Decentralized KYC Platform?

New technologies that enable decentralization may fundamentally change the corporate KYC approach. The most significant difference between centralized and decentralized solutions is that a centralized KYC utility is controlled and operated by a single entity. Blockchain technology

Table 2: Centralized KYC Utilities

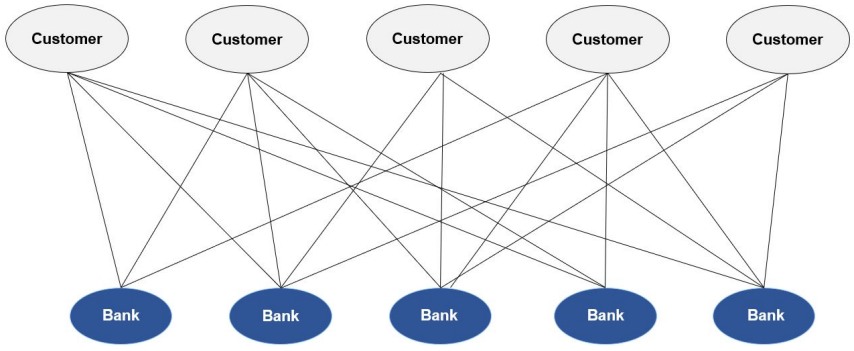
	Thomson Reuters	**Markit & Genpact**	**SWIFT**
Focus	Centralized repository for documentation and data	End-to-end management of company data and documents	Collection and distribution of bank KYC data
Target Market or Client	Corporate, Wealth Management, Institutional, Retail	Asset Managers, Hedge Funds, Corporates	Correspondent Banks
Key Bank Participants	Barclays, Goldman Sachs, Credit Suisse, JP Morgan, State Street	Citi, Deutsche Bank, HSBC, Morgan Stanley	Citi, JP Morgan, Deutsche Bank, HSBC
Geography	Global	US, UK	Global
Key Differentiation	Utilization of established data resources like World-Check	Partnership of deep expertise in technology and financial data	Data quality checking and data supplementation/enrichment

Source: Citibank 2014

can decentralize that control and operation — enabling entities to coordinate and agree upon information between each other, bilaterally or multilaterally, without concentration of processes or data through a single intermediary. By using a pre-agreed upon consensus algorithm, entities in a blockchain network can maintain collective records without trusting a third party. There also is not a need to retroactively reconcile information between disparate databases when there is a shared ledger ensuring a correct, current, consistent source of truth exists at all times.

Figure 2 demonstrates the decentralized approach. Each node has the potential to communicate with any other node in the network on a private peer to peer basis. With a decentralized corporate KYC platform, a direct customer-to-bank relationship would remain, without a central operator maintaining the platform and controlling information flows. Customer information would only be shared with the relevant parties necessary to satisfy the transactional requirements. Third parties, such as attesters of certain identity characteristics, could sign off on relevant facts, but would not have a holistic view of a corporate customer's identity profile.

Figure 2: Decentralized KYC Utility



Source: R3

Decentralization is a complex topic — the promise of blockchain technology involves decentralizing control across architectural, political, and logical spheres (Buterin, 2017). However, no network using blockchain technology is entirely decentralized, and different blockchain networks will have varying degrees of centralization and decentralization. For example, Bitcoin and Ethereum are examples of cryptocurrencies which are designed to be decentralized across the different spheres, but in some respects, are centralized (Azouvi et. al, 2018). In practice, complete decentralization, at its most extreme interpretation, is impossible and unrealistic (Gencer et. al, 2018).

Still, many enterprise use cases, including corporate KYC, can benefit from more decentralization. A shift towards more decentralization can reduce the risk concentrations of new intermediaries. Further, decentralization may protect against stagnant incumbents that stifle innovation or become rent-seeking once established. In the context of corporate KYC, there may be advantages for decentralization across operational resiliency (no central operator or point of failure), data security and privacy (direct customer-bank data sharing, avoidance of data "honeypots"), transparency, scalability, process flexibility, and others described in Section 3.

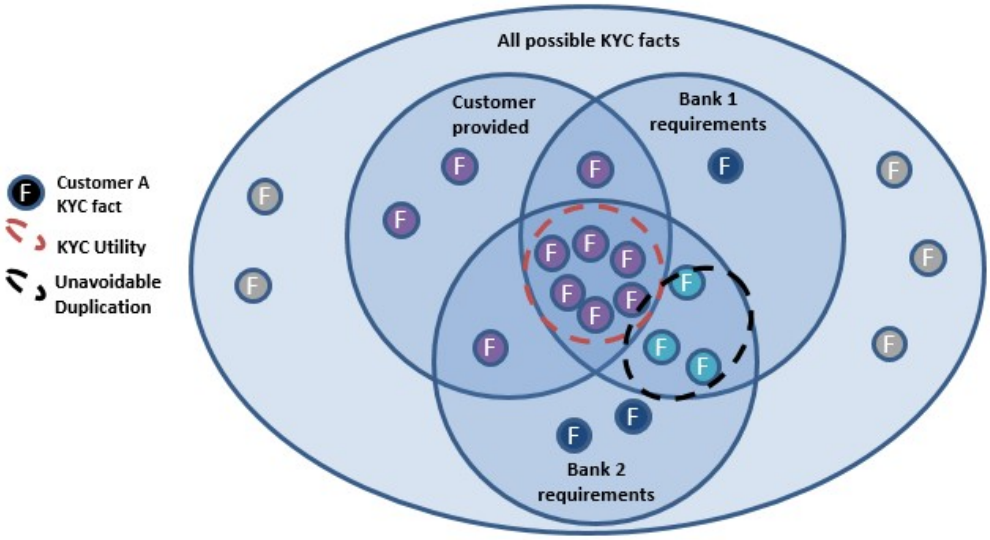
2.2 Decentralized KYC Platform Models

Initiatives across the blockchain space have experimented with several models for corporate KYC. The self-sovereign model, and the bank-sharing model are two basic archetypes.

KYC utilities or platforms intend to address the problems of redundant effort and process complexity. The information in any KYC solution would include the customer-provided KYC facts in the red circle in Figure 3. Additionally, a KYC platform also would also allow customer to provide information to specific banks.

The black circle shows redundant information that banks collect that is not customer provided, which has not historically been shared between banks.

Figure 3: KYC Utility or Platform Information

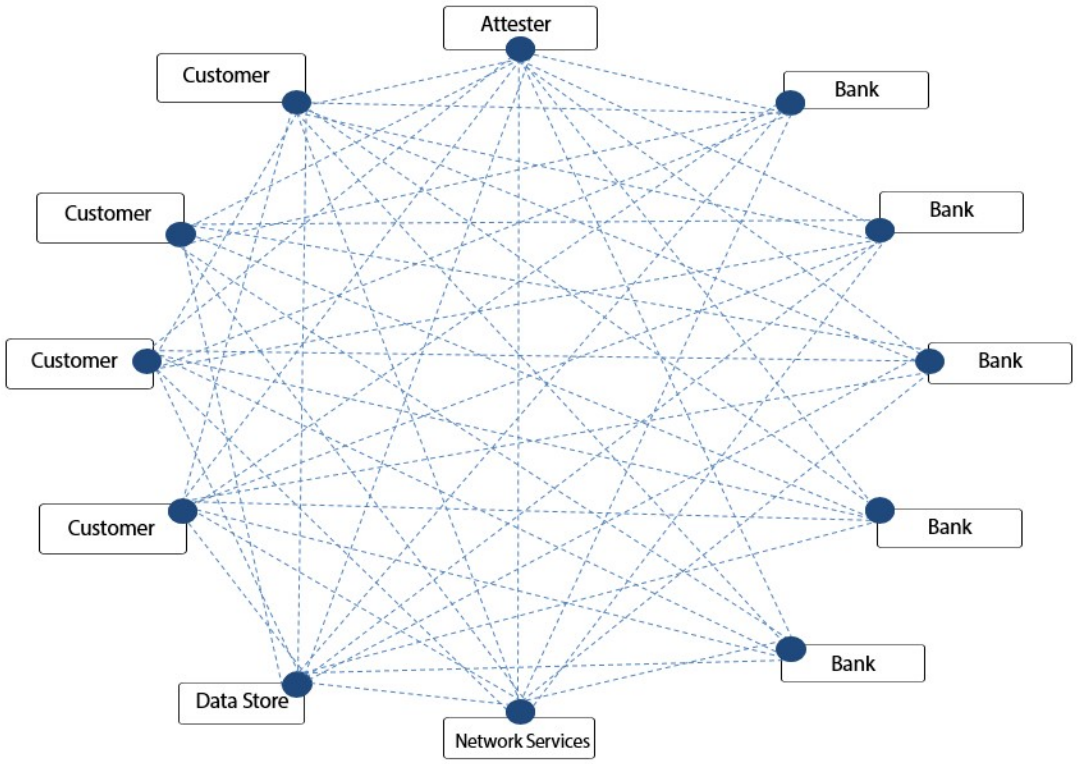


Source: R3

Self-Sovereign Model The self-sovereign model allows corporate customers to create and manage their own identities including relevant documentation and then grant permission to multiple participants to access this data. Each entity has the potential to communicate with any other entity in the network on a private peer to peer basis, as depicted in Figure 4, with the caveat that banks do not share customer data with each other. The self-sovereign model is significantly more likely to succeed in most jurisdictions, particularly due to customer data privacy conventions and regulations.

The relationship remains customer to bank, with the rights and responsibilities of each laid out in a contract. The bank doesn't control or necessarily store any of the customers data. Instead, the customer permissions the release of their data to each bank. If a customer has multiple receivers of their information, then it has multiple legal agreements, but they use the same data and mechanism to provide their KYC information to the various banks. Different attesters can provide network services on the platform to both customers and banks.

Figure 4: Entities Connected over the Internet, Communicating on a Peer-to-Peer Basis



Source: R3

The self-sovereign model is realistic because it would streamline data collection for the banks without introducing substantial new regulatory considerations. It also is aligned with regulatory tailwinds that support having individuals and companies with more control over their own data. This approach improves data collection, but ultimately each bank would still provide their own due diligence. Due diligence is the forming of an opinion as to whether the customer passes KYC/AML checks once they have received the customer data. Due diligence (and liability) for their customers would remain with each bank, and they would receive the fines for any non-compliant behavior of a particular customer.

Bank Sharing Model A bank sharing model is currently unlikely in most jurisdictions, and is the more disruptive and extreme of the two. The bank sharing model could be different from self-sovereign approach in two ways. The first is that, data collection by banks in theory might allow the black area, in addition to the red area in Figure 3, to be included in a KYC platform. This area includes both customer provided facts and also redundancies between banks that aren't customer provided. In some jurisdictions, such as the United States, banks cannot share customer data with other banks, while in others, such as Italy, they can. Shared data collections on customer data would raise some concerns over customer data privacy.

Second, there is a also, chance, in some markets, there will be a model where banks may share both data collection and due diligence between each other. This approach would be significant change from current practice and may not be realistic in the short term — though depending on implementation there are efficiency benefits. It would require some form of well-developed liability sharing framework amongst bank users of the platform and a significant structural and legal/regulatory lift. The bank sharing model would require a shared liability community agreement, such as the one formed by CAcert and IdenTrust. In the context of corporate KYC, an effective agreement would require a common mutual contract, suppliers of data to accept responsibility for data, community policies and practices, and a dispute resolution framework (King et. al 2016).

3 Is a More Decentralized Approach a Better Way?

This section describes the benefits of a decentralized KYC platform relative to existing centralized approaches, describes common obstacles faced by both centralized and decentralized KYC, and discusses novel problems that decentralized systems introduce.

3.1 Benefits of Decentralized KYC Platforms

Retain Direct Customer-Bank Data Sharing Relationship With the centralized KYC utilities that launched in 2014-2015, introducing a third party created new questions regarding trust with regards to customer data privacy and control.

KYC utilities that are centralized require the intermediary to:

- **Use data appropriately:** Banks and customers trust that the central entity will not monetize the data for other purposes not connected to the delivery of the KYC service.
- **Correctly manage permissions and access:** Banks and customers trust that the central entity will manage permissions and access as legally agreed and without accident.
- **Keep data secure:** Banks and customers trust that the central entity will adequately protect customers' data. A centralized KYC utility is a "honeypot" for hackers, and confidential data may be less secure outside a bank, forming a new potential vulnerability.

More Operational Control A key issue with centralized KYC is that they add a new interim third party operator between the customer and the bank, creating an important central point of failure. Banks and customers must trust that the central entity will operate reliability and sacrifice operational control over parts of the data providing and collection process. A decentralized system would be more resilient. There would be operational risks but they would be bilateral or between particular nodes, and not the whole responsibility of a single third party provider.

More Transparency Ideally, a decentralized platform would link customers to banks directly. For both parties, "what one sees is what the other sees." There would be increased transparency for both the customer and the bank due to the shared logic and shared states between their nodes on-ledger, both for static data and evolving data. There would no longer be a need for customers or banks to consult an intermediary to understand who has what information regarding the parts of an application. Further, both parties could more easily check directly between each other where both sides are in the process with fewer manual confirms.

Flexible Processes Centralized utilities add another step in the linear processing of information. Decentralized platforms allow for a flexible, flattened, and non-linear process, without bottlenecks. For example, a customer's single update could propagate simultaneously to all authorized recipients of the data, and both the customer and relevant banks can confirm that it has happened instantly. This may reduce duplication by the customers who have to send updates repetitively to each bank they engage with. For banks, it would provide a standardized process for all customers which will automatically feed customer updates when they occur.

Easier and Automatable Attestation A system based on blockchain technology could streamline the attestation process for data providers and relevant third parties. Multiple authoritative parties on ledger could attest to specific facts regarding the corporate customer. These attestations could allow a bank to gain a holistic profile on a customer, not through static record gathering, but from a more dynamic attestation model from sources network-wide.

Decentralized KYC platforms favor such relationship-based attestations over centralized aggregations of information. This approach would more closely resembles a dynamic peer-to-peer network of relationship-based identity characteristics being shared based upon context and attestations, rather than reliance upon authorities that collect data to form a static profile on a particular legal identity (Grigg 2017).[1]

[1] Ian Grigg best describes this approach in the R3 Report "Identity in Depth": "What is valuable is not the node but the relationships that we can examine and record between any two given nodes. It helps to think of the node - the person - as a blank circle, and then imagine in your mind's eye tracing the relationships between the circles."

Scalability No single company could gather information about all corporate customers across an entire economy and ensure that the relevant information is up to date and accurate. The decentralized approach is more scalable because effort remains spread out amongst customers and banks. A relationship-based attestation and submission network is more scalable than a centralized store of information.

Customer Data Protection Blockchain technology fosters customer data sovereignty and can help put customers in charge of their own identity data. Customers can take greater ownership and control over who has permission to access and use their data across the financial services industry. The customer can manage the creation, update, and availability of data to various parties according to the type of business the customer wants to undertake. These developments are aligned with growing movements and public debates regarding data privacy, in the wake of data privacy scandals, hacks, and misuse, that have led to GDPR-type regulations.

3.2 Common Obstacles Faced by Both Centralized and Decentralized KYC

Standardization Globally there is a lack of common identity data standards and information requirements. In some jurisdictions, prescriptive regulations determine standards, while in others, regulators provide guidance and leave banks to develop their own best practices. This means that different banks often have different processes and standards, which can cause complexity for corporate customers.

The financial industry requires clear minimum quality standards applicable to both the makers of facts and to the users of the facts. Such a standard would require industry-wide agreement. Well documented and auditable standards simplify processes for providers of data.

Pre-Ledger Complexity (Digital Modernization) The format of identity documentation is out of both the customers' and the banks' control. No matter the technology of a KYC solution, most governments still use paper-based identification documents, and those documents are often necessary within the KYC process. Any electronic transmission of identity information needs to ensure that data is in the correct format.

Post-Ledger Complexity (Internal Bank Complexity) Having a shared and reliable source of information from a KYC solution can help facilitate agreement on facts for banks but will not address internal complexity specific to that bank. Many of the costs and delays with corporate KYC are due to internal bank processes, communication, and alignment. Banks have significant technical and operational challenges with developing a consistent, enterprise-wide view of customers' information. To respond, banks have developed new enterprise or master data management initiatives to overcome the fragmented nature of many internal customer databases, but there remains fragmentation.

Integration Enterprise software requires integration. Integration is often a barrier to entry for new products at banks. This barrier remains whether the software is centralized or decentralized.

Incumbent Involvement There are significant barriers to entry with launching a corporate KYC solution. New financial market infrastructures, particularly those of systemic importance, often require a consortium approach and a large number of relationships with banks. Centralized KYC utilities were launched by incumbents within financial services, particularly data providers (Thomson Reuters, Markit), established market infrastructures (DTCC). New consortiums with banks are likely necessary to drive a decentralized KYC platform.

Critical Mass Part of the difficulties that centralized corporate KYC utilities currently face is that there are competing solutions, which means that customer data is segmented and siloed across separate databases. The variety of identity service providers and client data utilities have led to competing identity schemas and identifiers.

For a decentralized corporate KYC platform to be most effective, the financial services industry would need to consolidate around a single solution to avoid complications from cross-platform data transfer. It is much easier technically to move information within a single platform than across

different platforms, whether the solution is centralized or decentralized. A plethora of offerings as the decentralized corporate KYC industry matures would likely lead to their failure.

Underappreciating the difficulty of cross-platform interoperability, no matter the underlying technology, will ultimately risk a rebuild of the siloed financial market infrastructure in place today.

3.3 Novel Challenges for Decentralized KYC Platforms

Novel Data Privacy Issues Many public cryptocurrencies use a proof-of-work consensus which propagates all information to all nodes. Blockchains with a public broadcast approach to data privacy are inappropriate platforms for a corporate KYC use case that requires strict customer confidentiality and privacy. Given the consent of the customer, customer information should only be shared with the relevant parties necessary to meet KYC requirements. Therefore, a corporate KYC platform would need to be built upon an enterprise blockchain technology system that emphasizes privacy regarding information sharing.[2]

Network Governance Enterprise blockchains avoid the public twitter-fueled decentralized chaos that many cryptocurrencies face with governance of their respective platforms. Still, governance of enterprise blockchain networks, particularly for applications that require coordination amongst many different firms, is no small feat.

Enterprise blockchain networks require governance for technical, business, and legal dispute resolution frameworks. Technical governance will involve technical direction for the development of the platform, interoperability standards, reviewing and maintaining security and privacy against attack, and ensuring operability (such as scalability, availability, and monitoring). The business governance will require the ability to ensure the ongoing operation of the ledger, assessing whether it is achieving its goals, driving efficiency. Further, the creation and maintenance of these agreements will require a legal governance function. There should be some enforcement mechanism to ensure compliance with legal and regulatory requirements (Oldfield et. al, 2016). There have been many different existing governance models with consortiums in financial services, such as SWIFT, CLS, Markit, EBS, CHIPs, that may be leveraged with the corporate KYC approach.

Novel Regulatory Changes Centralized utilities faced legal and regulatory hurdles, and decentralized approaches will as well. Currently, there is no well-developed legal framework that governs and supports the use of decentralized networks based on blockchain technology to manage identities.

Bank confidentiality and data privacy laws affect different jurisdictions differently. For example, for any potential cross-border implementations, several jurisdictions mandate that identity information must be stored and controlled with the country, such as Luxembourg and Singapore.

Currently, banks are entirely held accountable by regulators and customers for abiding with the law and regulation. There are certain approaches, such a corporate KYC platform using the bank sharing model, that would require an advanced form of regulatory liability sharing or mutualization framework.

4 Conclusion

Are the same problems that limit centralized utilities also going to limit decentralized platforms? There are certainly common barriers, and decentralized technologies also introduce their own unique issues. Given that many problems remain with corporate KYC despite the introduction of centralized KYC utilities, a new technology that enables a decentralized approach for existing problems is worth using. A decentralized platform would address several of the key shortcomings that centralized utilities bring by retaining a direct customer-bank approach, giving more

[2]There are various architectures of a KYC platform that are possible. Currently, in the enterprise blockchain space, only Corda begins with point-to-point messaging, avoiding the architectural complications that come from forking or adjusting public broadcast blockchain architectures. This makes it the best fit for designs that consist of complex privacy rules and relationships between customers and banks.

operational control to banks and customers, more transparency, flexible processes, easier and automatable attestation, greater scalability, and by aligning with customer data protection regulatory tailwinds.

Any realistic corporate KYC solution requires substantial resource, relationships, and buy-in from a broad industry-wide effort. As a point of reference, centralized utilities were launched by firmly established entities in financial services, such as SWIFT, Depository Trust & Clearing Corporation (DTCC), Markit-Genpact, and Thomson Reuters. An organization would ultimately need to have a similar reach in order to address an issue of this breadth and complexity.

Because of these barriers to innovation, a consortium-based approach is likely. Project CordaKYC was a recent early stage consortium-based effort with 39 firms communicated and managed test customer KYC data across 19 countries across eight time zones in Microsoft Azure. As these efforts and others across the blockchain space mature, the financial services industry should consolidate around the corporate KYC use case to ensure alignment.

Identity is at the core of many banking problems, from financial inclusion to cross border trade and payment flow restrictions. The growth of blockchain technology has triggered new ways of thinking about and approaching identity, and decentralized corporate KYC is off to a promising start. Even marginal improvements with identity and KYC processes by leveraging advances in technology could have global implications for the fluidity of commerce, the availability of funding, and broader global access to financial services. Corporate KYC presents a complex and difficult problem, but it is one that causes enough collective friction and inefficiency that it is worth trying again to solve.

References

Azouvi, Sarah, Mary Maller, and Sarah Meiklejohn. 2018. “Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance.” https://fc18.ifca.ai/bitcoin/papers/bitcoin18-final13.pdf.

Buterin, Vitalik. 2017. “The Meaning of Decentralization.” Blog post. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

Buterin, Vitalik. 2016. "Chain Interoperability." R3 Report. https://www.r3.com/research/.

Citi. 2014. “Know Your Customer Utilities.” Treasury and Trade Solutions. http://www.citibank.com/transactionservices/home/sa/cab/meetings/documents/2014_armonk/1264378_gts26449_know_your_customer.pdf.

Gencer, Adem Efe, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer. 2018. “Decentralization in Bitcoin and Ethereum Networks.” https://arxiv.org/abs/1801.03998.

Grigg, Ian. 2016. "Identity in Depth." R3 Report. https://www.r3.com/research/.

International Chamber of Commerce. 2018. “Global Survey Report.” https://iccwbo.org/publication/global-trade-securing-future-growth/.

King, Nigel, Nick Skinner, Ian Grigg, Stephen Lane-Smith, Atefeh Mashatan, Craig Maladra, John Vondrachek, Paul Bayer, Christopher Swanson, Henry Roxas, and Abbas Ali. 2016. “Foundations of DLT: Identity.” R3 Report. https://www.r3.com/research/. Private Access: https://r3-cev.atlassian.net/wiki/spaces/RP/overview.

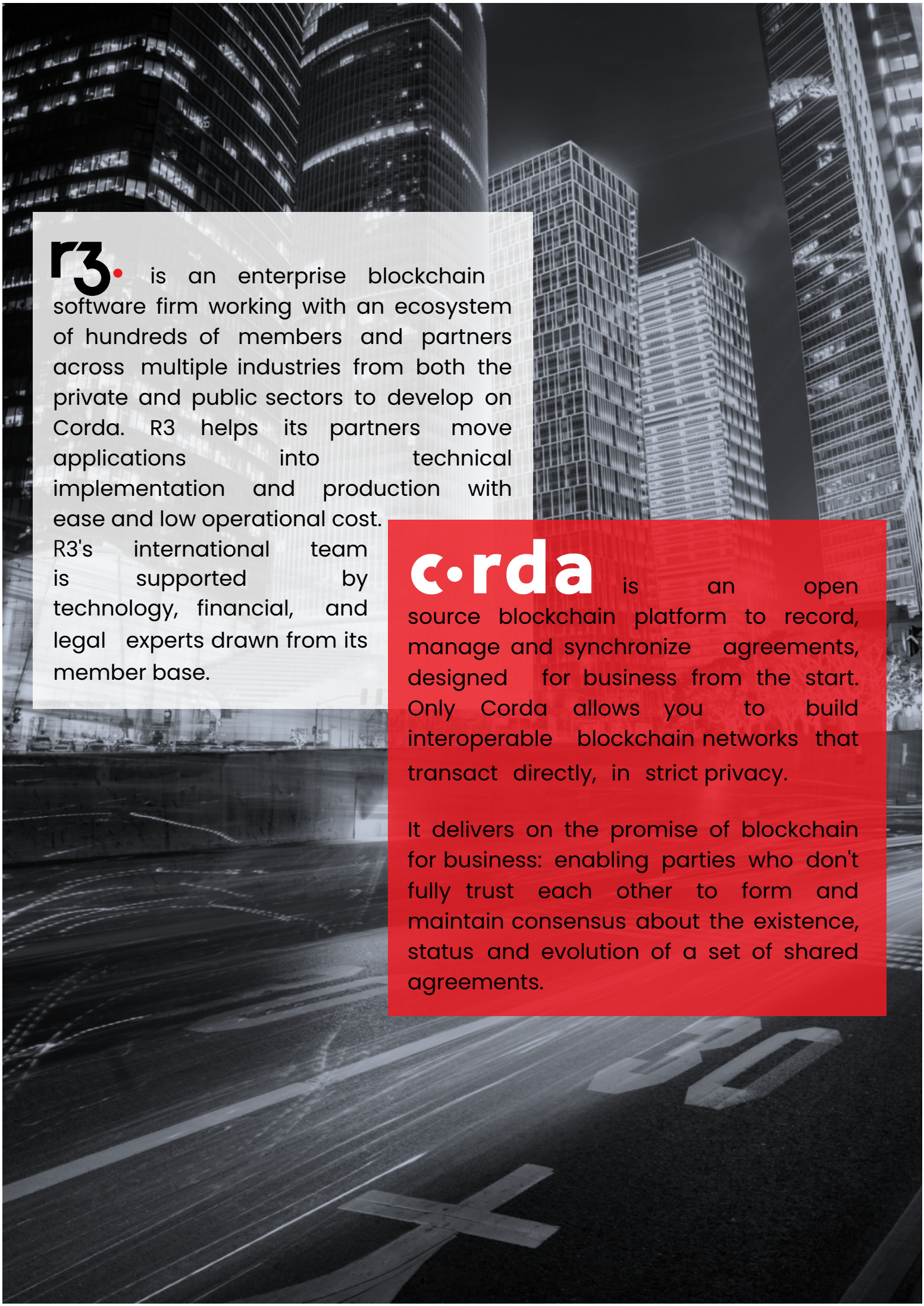
Oldfield, Mark and Stephen Lane-Smith. 2016. “Foundations of DLT: Non-functional Considerations.” R3 Report. https://www.r3.com/research/. Private Access: https://r3-cev.atlassian.net/wiki/spaces/RP/pages/128595136/Non-functional+Considerations.

Patel, Neepa. 2017. "Blockchain KYC/AML Utilities for International Payments: A Regulatory Solution for Anti-Money Laundering and Financial Inclusion?." R3 Report. https://www.r3.com/research/.

Ray, Arin and Cubillas Ding. 2014. “Emergence of a Utility Model: The Case of KYC On-Boarding Solutions” Celent. https://www.celent.com/insights/359447025.

Rutter, Kevin. 2017. "The Myth of Easy Interoperability." R3 Report. https://www.r3.com/research/.

Thomson Reuters. 2017. “KYC compliance: the rising challenge for financial institutions.” Survey. https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/report/kyc-compliance-the-rising-challenge-for-financial-institutions.pdf.



R3 is an enterprise blockchain software firm working with an ecosystem of hundreds of members and partners across multiple industries from both the private and public sectors to develop on Corda. R3 helps its partners move applications into technical implementation and production with ease and low operational cost. R3's international team is supported by technology, financial, and legal experts drawn from its member base.

Corda is an open source blockchain platform to record, manage and synchronize agreements, designed for business from the start. Only Corda allows you to build interoperable blockchain networks that transact directly, in strict privacy.

It delivers on the promise of blockchain for business: enabling parties who don't fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared agreements.