Blockchain for Financial Services—Implications, Challenges, and Opportunities

Sean Stein Smith

Following the rise in prices of bitcoin and cryptocurrencies in 2017, interest and investment in the underlying technology, blockchain, has continued to rise virtually unabated even as the prices for bitcoin and other cryptocurrencies remain depressed from previous highs. The appeal of blockchain for enterprise applications tends to be concentrated around the fundamental technical characteristics of how the technology itself functions. Even with the regulatory uncertainty and technical complexity that continues to be associated with enterprise or commercial adoption, investment continues to increase. Both in terms of financial resources and people hours, investments and allocations of resources continue to become increasingly mainstream across an array of industry verticals. While there are multiple implementations underway across any number of economic sectors, the purpose of this analysis focuses on financial services applications. Given the fact that the original bitcoin blockchain was, in large part, developed to decentralize and democratize the current financial system, the current pace of adoption by incumbent financial actors is a source of continued analysis and debate between market actors. Regulatory pushback and scrutiny of projects such as Libra are indicative of the dual nature of this increased interest in blockchain for commercial purposes; as large organizations develop blockchain options, they are increasingly facing regulatory hurdles.

Without spending excess time focused on technical jargon, the following characteristics seem to be the driving force behind the appeal, interest, and investment in blockchain tools. With billions of dollars invested and hundreds of projects currently underway in the space, it would be easy to lose track of the fundamental characteristics that make blockchain appealing to enterprises across industry lines. No matter what specific project is being analyzed, the core characteristics of blockchain represent the focus of both the analysis of blockchain itself as well as the individual projects underway. Framing the conversation to be explored in more depth throughout this piece, the following considerations appear to be especially
Blockchain Core Characteristics

1. Encryption lies at the core of the blockchain ecosystem, as opposed to simply being added as either an afterthought or post-production tool, helping to better secure and encrypt sensitive data across different industry sectors.

2. Blockchain seeks to address gaps in current centralized and distributed methods of storing and sharing data, namely weaknesses associated with access and password policies.

3. Scalability, while an issue for public blockchains using a Proof of Work (PoW) consensus methodology, seems to be addressable if an alternative consensus methodology is implemented.

4. Multinational enterprises, now including large financial and information technology players, are offering blockchain-as-a-service offerings for various entities to adopt and utilize.

5. Costs and usability are both issues increasingly addressed as different iterations of blockchain and blockchain augmented platforms by emphasizing different options than those used on public blockchains.

Consensus

Arguably the most unique characteristic of blockchain technology is the consensus mechanism by which data is validated, confirmed, and ultimately added to the blockchain itself. What this means from a practical and implementation focused approach is as follows: no single member, be it an individual or institution, can unilaterally add, edit, or otherwise add information to the blockchain. Such an approach is core to the decentralized and distributed nature of how blockchain iterations interact with existing data management systems as well as other emerging technologies. There are a variety of specific consensus methodologies that can be implemented by an organization or group of organizations depending on the desired outcome, but at the core of the idea, there are several characteristics that are consistent across the board.

The first attribute and associated strength of a consensus-based methodology is that, as a result, every network member—if they are a full node or otherwise designated as recipients of the entire record—receives an up-to-date record of the transactional data that has been stored on the blockchain. From a financial services perspective, this real-time updating of information allows for greater transparency and traceability into the records themselves, as well as additional protection against fraud. Since network members have full records that have, in essence, been approved by the network itself, the process of comparing this data to outside or third-party data becomes a more streamlined and simpler process. Building on this first strength, every block—and the transactional data contained therein—must have previously been approved by some percentage of network membership. Specifics may vary, but ultimately each and every piece of data recorded and stored on a blockchain was approved by a group of network members, lowering the risk of one or even a group of malicious actors from seizing control. Thirdly, the embedding of hash identifiers
into each block and making each subsequent hash ID related to the one immediately preceding it, make it exceedingly difficult, if not impossible, to alter records after they have been added. Analyzed from a financial services perspective, this creates an almost continuous audit trail that can be used by forensic experts, external audits, process improvement specialists improved within the firm, or anyone else focused on ensuring that the data reported externally is uncorrupted and accurate.

Two additional core attributes and strengths of the consensus methodology link directly back to the core functionality of blockchain itself. At the center of the idea, a blockchain is a decentralized and distributed ledger, or record, that network members can use to store and transmit data in a manner that has proven very resistant to hacking and other cyberattacks. This resistance, however, is not simply due to the decentralized and distributed nature of the ledger itself; simply storing data in multiple places does not inherently increase the security of that information. In addition to the group-based approval of transactions and blocks prior to approval, encryption provides an additional layer of security and integrity for all information stored on the blockchain itself. This combination of encrypted data that is updated as new transactions and blocks are added to the chain and the fact that this record is stored in a large number of different areas creates a network extremely resistant to DOS or other volume-based attacks. Even if one, or many, nodes were to fail or go offline for a certain period of time, the network would still be able to function due to the distributed nature of the records stored on this platform. Various consensus options will be examined throughout this piece, including a compare/contrast, but the general principles outlined above will apply to all subsequently listed options.

Organizational Adoption

Perhaps the most logical place to begin the analysis of blockchain’s applicability for financial services and infrastructure development is to not only identify the core components of blockchain technology, but to also identify how these components differ from traditional and current computing options. After these core components have been established and defined, this analysis can then pivot and shift to the types of blockchains available for organizational adoption.

First, while recent hacks and data breaches have reduced the aura of invincibility that once surrounded blockchain, the concept and idea of immutability still seems to remain a valid way to think of the platform as a secure method of storing and transmitting information. From an enterprise application, it is more logical to think of the security and data integrity connected to blockchain as being tamper-resistant. In traditional database structure, unauthorized access can result in edits or changes to customer, client, or institutional records that may or may not be discovered in a timely manner. Contrasting this with the tamper-resistant nature of blockchain, which will be analyzed in more depth below, the consensus-based way in which data is added, stored, and communicated via blockchain is a differentiating factor. From an application perspective, this means that—as long as the coding and programming are done correctly—no one single actor or institution will be able to make unauthorized changes to records and information.

Second, the related components of traceability and transparency are linked directly to the core value proposition of blockchain, both as it stands on its own and relates to current data technologies. Cloud computing is often touted as the next stage in enterprise adoption of computing software solutions and has created an entire industry of service providers and consultants to facilitate the adoption and implementation of this technology. That said, simply using a cloud-hosted service does not increase the traceability of where information is coming from or the transparency regarding when and how certain pieces of information are added to the blockchain. Sharing information among partner organizations, conversely, can reduce the transparency and traceability connected to network data due to the increased number of participants,
varying control and custody policies, and lack of standards for data formatting and access. Blockchain, it is
ture, also relies on the idea of a decentralized platform to store and transmit information, but this decen-
tralized concept is augmented with encryption and consensus methodologies.

Third and finally, the encryption that is embedded as a core component of a blockchain network differenti-
ates it from either a centralized data management platform or a decentralized cloud-based computing
network. For example, in a centralized network model, there is only one voice driving the conversation as
it connects to data management policies, access rights, and how the network is updated over time. This can
lead to policies that are inapplicable for a majority of network members; changes that are implemented in
a patchwork manner; and increased exposure for hacks, breaches, and other data leaks. Cloud-based solu-
tions may actually compound this problem by spreading the information and data stored on the network
between network members without, in many cases, any way to preserve security over the information,
consistent application of data controls, or enforcement of network upgrades. Blockchain, contrasted to
both of these existing options, has encryption and data security at the core of the idea, rather than simply
added on as an aftermarket component.

Consensus Drilldown and Differentiation

Different blockchain options and models use different consensus methodologies, and having a firm un-
derstanding of some of these different models represents another consideration that organizations and
leadership teams should analyze prior to implementation.

Proof of Work (PoW)—The PoW model is the model of consensus that underpins, perhaps most famously,
the bitcoin blockchain and is also the methodology that requires the most computational and electrical
resources to be implemented effectively. Under this methodology, for any new block to be added to the
chain, miners (also known as full nodes) must solve a mathematical puzzle to quantitatively link the block
presented for approval and validation to the previous block. Once this math puzzle has been solved, other
miners verify the legitimacy of the solution and the block is added to the existing blockchain. The SHA-
256 bit encryption is utilized by the bitcoin blockchain in addition to the PoW consensus methodology,
which was actually initially developed by the NSA, and which to date has proved to be unhackable. From
an enterprise perspective, however, the complexity, energy required, and time delay that this methodolo-
gy results in make it less than optimal for commercialization. Instead, proof of stake has emerged as one
viable alternative.

Proof of Stake (PoS)—The idea underlying the proof of stake consensus methodology is a concept that
is both intuitive in nature and helps to address some of the fundamental issues connected to PoW. In
essence, what this methodology seeks to leverage is the following: if an organization or group of organi-
izations have an ownership level—or stake—in the blockchain, they are going to be more likely to work to
maintain the validity of the blockchain. In a public blockchain situation, this is most likely not applicable
due to the sheer volume of network members, but in a private or consortium construct, this may be more
appropriate. For example, if a private blockchain network consists of 20 members, the 5 largest—in terms
of network investment or other forms of ownership—may be designated as those parties primarily re-
sponsible for data approval and entry. Although this does concentrate the data approval process, it does so
between network members with the most at stake (hence the name).

Questions that are quite often asked at this stage in the conversation are just how PoW and PoS are dif-
ferent from a logistic basis, why PoS may be faster, and why PoS may be a more appropriate fit for organi-
izations seeking enterprise adoptions and options. In essence, instead of every full node racing to solve a
math puzzle and then waiting for a specified number of other nodes to verify the solution—all of which can bog down the data validation process. PoS works on a voting based on how much of the network a particular individual or institution owns or how large their “stake” in the network actually is. In addition to making it simpler for members to see how information is being approved, this also has the added benefit of more efficiently allocating resources because members are not competing and racing to approve every individual block of data.

Delegated Proof of Stake—An offshoot of PoS, the name of this consensus methodology appears to be more complicated and abstract than it may be in reality. Operating under the same basic assumption as proxy voting does for other corporate governance activities and actions, the delegated proof of stake may be the appropriate methodology for a blockchain with a relatively smaller number of larger members but a large population of smaller members. Especially as blockchains are implemented between organizations operating on a global basis, it may be logical for smaller entities to delegate voting rights and authority to larger and more established network members. On the spectrum of low trust to high trust, the delegated proof of stake would work best—and be most appropriate—for a higher trust or higher familiarity environment than would be supported with a PoW methodology. This is because the very fact that voting rights are delegated would seem to indicate a higher level of trust and transparency between network members.

Arguably the most important differentiating factor between blockchain technology options and other existing technology tools is how the specific consensus methodology underpinning a specific blockchain functions. Again, the primary enterprise takeaway is that—as stated in the name of the methodology itself—no one single individual or entity will have the ability to edit or change the data stored on the blockchain. Drilling down into how the different consensus methodologies work but by no means presenting an all-inclusive listing, the preceding methods seem to be the most relevant for this analysis. Regardless of the specific methodology selected, it is important to acknowledge the fact that this concept underpins the entire blockchain ecosystem. Attempting to not dwell overly so on this topic, the consensus model underpinning virtually all blockchain platforms means that, in order for data to be uploaded at all, multiple parties must confirm its veracity. Bitcoin, and the bitcoin blockchain itself, utilize the proof of work consensus methodology, which has proven resistant to hacks as of this writing. As is discussed in more depth, however, this methodology may not always be practical or appropriate for the enterprise applications being discussed. Different protocols require different levels of verification, so it is important to understand which model is appropriate for a given situation and the factors that should be a part of any external analysis. The different consensus methodologies also connect and build on the conversations and considerations linked to the specific blockchain iteration selected by an organization.

**Different Blockchain Options**

Particularly for business practitioners seeking to implement or evaluate the validity of blockchain options for enterprise utilization, there needs to be a conversation linked to what type of blockchain will be put into practice. Blockchain may be a word that financial professionals are familiar with, but there are different options that are going to be a better or worse fit than others depending on the enterprise. Prior to drilling down into what some of the implementation opportunities and challenges are, it seems logical to break down the word blockchain into the two general buckets that, until recently, led the technical and implementation sides of the conversation.

1. Public/permissionless blockchain—this is the model and platform of blockchain that was first introduced to the marketplace, and it is the type of model that underpins cryptocurrencies such as bitcoin and ether. From an enterprise perspective, however, this may not seem like the most
appropriate model due to the computing and electrical requirements it uses to process and validate transactions (under the PoW methodology). This has led to the development and implementation of other types of blockchain solutions in the marketplace, namely the rise of private, public-permissioned, or other federated models of blockchain.

a. Given the open-access nature of a public blockchain and the fact that literally anyone can join this network, the PoW consensus methodology is most commonly used to validate transactions with this model. For financial services, however, public blockchains may not be optimal for a number of reasons. First, the cost and technical complexity of implementing is compounded by the reality that—at the end of the day—all data and transactions are posted on the public blockchain. For most commercial or governmental enterprises, this is not an ideal scenario. Second, implementing, maintaining, and integrating a public blockchain basis of storing and transmitting data is cost-prohibitive given the computing, electrical, and operational complexity needed to commercialize a public blockchain option. These, among other issues, have led to a pivot and shift in the broader ecosystem, specifically the rise of private or federated blockchain models.

2. Private/permissioned or federated models of blockchain, on the one hand, may be simpler to implement and use from an enterprise perspective due to the fact that these models need not use the PoW consensus methodology. Specifically, the consensus methodology of data approval and posting is not usually the PoW model (while currently the most secure, it is also the most energy-intensive), but rather an alternative that is more applicable for a higher trust environment such as an enterprise situation. This model and type of blockchain represents the model and option most commonly implemented by organizations seeking to integrate this emerging technology with current technology tools.

a. Taking into account the needs of enterprises seeking to adopt blockchain for data processing, storage, and transmission, it is increasingly evident that a private, consortium, or federated model of blockchain would appear to be most appropriate. Such a decision seems to be more practical for two reasons. First, the higher level of trust embedded into a consortium or private model means that the energy and computational power is less. This means that it is cheaper and less expensive to implement this model of blockchain than a public blockchain, which is clearly a primary decision driver for enterprises. Second, this model of blockchain—amplifying the encryption and transmission of data between organizations that are already familiar with each other—mirrors the search for efficiency present in every organization. A private, consortium, or federated model of blockchain would appear—given current iterations—to be the more practical model for commercial adoption.

b. Given the higher level of trust and transparency with regards to who exactly is a part of the network, private blockchains can use alternative consensus methodologies to improve the efficiency of transactional processing.

Perhaps one of the most significant individual benefits that can be achieved via the implementation of blockchain-based solutions is the combination of ecosystem speed and security with which data is transmitted and communicated between network members. Blockchain, regardless of the specific option that is implemented at the organization, has security and data integrity as the primary functionality of the system—removing the need for intermediaries—instead of other functionality such as processing speed or superior graphical interfaces. When referring to the speed with which blockchain-based transactions can be completed, it is important to specify what category of transactional processing is referenced.
While it is true that many blockchain options, at least as of this writing, do not process transactions or information at the same speed as traditional centralized options, it is important to realize the primary reason for this discrepancy lies at the core of blockchain itself. In any transaction, whether it takes place in a financial services context servicing credit cards or the settlement of equity trades, there are always two components to the transaction. DLT arrangements may take longer to achieve settlement, at least initially, than with the current iterations of real-time gross settlement systems due to the increased complexity of processing and approval at the core of how blockchains function. While surface-level processing of transactions and block approvals may be slower via a blockchain platform, the final reconciliation and settlements accelerate due to the continuous verification and sharing of information between network members. In other words, the processing infrastructure may be slower in terms of settling individual transactions or pieces of data between organizations interacting on a one-to-one basis. Bringing this concept to a logical conclusion, the argument can, has been made, and should be made that friction across an ecosystem or value chain can ultimately be reduced if members are part of a common blockchain platform.

**Blockchain for Enterprise**

Building on the reality that, for the majority of enterprises and business transactions, a public blockchain is neither feasible nor practical, the development and pivot toward an enterprise model of blockchain would seem logical to forecast to continue. This raises, in a rather straightforward manner, the question of where an enterprise blockchain model fits in the context of technology and organizational solutions. More specifically, a question that is increasingly being asked—and answered—is how blockchain is superior and/or applicable for commercial applications and use cases.

**Where Does an Enterprise Model Fit?**

It is also important to remember that blockchain, in and of itself, does not represent an intuitively new technology nor even a particularly innovative type of data management and communication. Rather, acknowledging the reality that the implications and use cases of blockchain may be new, a logical way of viewing the technology is a logical iteration and next step in terms of how data is processed, stored, and transmitted. In essence, there are three basic models of data management that seem specifically applicable to both financial services and energy infrastructure and drive the conversation toward an enterprise blockchain model of doing business. The first kind of database structure, a centralized clearinghouse, is what tends to be most prevalent in either a financial institution setting or an infrastructure management situation. A centralized clearinghouse of storing and transmitting information between parties plays the role of gatekeeper, approver, and validator of data. Contrasting this centralized model of processing and approving data, a blockchain implementation is based on the sharing and collaborative efforts between network members. Stated another way, financial services institutions and networks, which rely on the continuous and collaborative transmission and utilization of data, provide a uniquely appropriate use case for blockchain platforms. Highlighted previously, the benefits of blockchain, with a continuous sharing of data and encryption providing additional security over this data, seem to provide a viable alternative to current data management solutions. Depending on the specific type of data in question, the central authority or organization may grant levels of access, allow different users to post or edit information, or serve a role akin to data custodian. Maintaining control over both the data itself as well as the levels of access that are granted to end-users concentrates both the opportunities and challenges connected to that role.

The benefits tend to be clear, including the increased efficiency and lower costs that come with a centralized hub, but the single point of failure has been shown time and time again to be a ripe target for hackers.
and other data-focused criminals to attack. Simply distributing the ledger and storage of information—such as what occurs in a cloud-based environment—does not improve the situation, as a primary result of that is that the information now must be protected and updated across multiple data services and platforms. As far as implementation and how a distributed or cloud-based data management system would function, the primary difference lies with how access and restrictions connected to the data would be stored in this set. In a cloud-based environment, there is the ability or authority to upload, edit, or otherwise modify information stored in the database. What this means, however, is that there may be multiple copies or versions of the same record depending on which individual or institutions access the data at any given moment.

Blockchain, and specifically an enterprise blockchain (which or may not more closely resemble a public-permissioned, consortium, or other private model), combines the benefits of both applications while reducing the risk to data integrity and management. Emphasizing these benefits and business applications is essential to understanding the costs and other implications associated with the development and implementation of such a model.

**How Enterprise Models Work & Can Be Implemented**

Prior to drilling down into some specific use cases of how an enterprise blockchain model can be put into place and benefit an organization, it seems logical to also analyze some of the headwinds that can stall or delay implementation. Costs, both related to the initial investment and the hiring necessary to staff the appropriate levels of technical talent, have proven to be prohibitive for all but the largest of organizations. Such costs also include the costs and funding necessary to maintain such a system after it has been installed. Additional considerations that need to be taken into account when developing and implementing a blockchain model include 1) the training and education of employees that must occur to ensure these platforms and technologies are utilized effectively, as well as the compliance issues that should be built into any blockchain analysis, and 2) the technical complexity that will accompany even the most straightforward implementation project.

Technical complexity is, of course, a challenge and an obstacle that should be taken into account when developing blockchain-based solutions, but it is also something that needs to be understood in the context of broader market developments. Time and again, sensitive information that had been entrusted to a central clearinghouse or intermediary has ended up being exposed, hacked, breached, or otherwise compromised and exposed to the wider public. As a direct result of these continued breaches of both technical compliance and consumer trust, regulatory agencies across the world have become increasingly interested in the protection and security of critical data. In other words, it is becoming increasingly clear that either organizations will discover a better way to store and transmit sensitive data or regulators will find one for them. For the purposes of this analysis, these trends and foci center around financial and infrastructure information but could logically be applied to virtually any industry sector.

**Control and Custody Considerations**

As enterprise blockchains continue to be considered and weighed as possible options for organizations across industry lines, it is important to connect some of the benefits and potential risks of doing so. Benefits, highlighted by the projects that have been implemented to date in both financial services and the public sector, include but are not limited to reduced latency (processing time in the system), lower time delays and friction, improved security and enhanced data integrity, and increased transparency and accessibility to organizational data. Several examples of financial services organizations that have successfully implemented blockchain include, but are not limited to, the following:
1. Allianz and AXA have both introduced blockchain services that deliver real-time updates and payments to customers who have suffered travel cancellations or after a flight or other trip has been delayed longer than a set amount of time.

2. BBVA, the second largest bank in Spain, recently announced a $170 blockchain-based syndicated loan. With loan syndication totaling trillions annually, the opportunities for savings via greater efficiency seem significant.

3. The volume credit derivatives operations of the DTCC, which handles trillions of dollars settlements annually, is transitioning to a private blockchain called AxCore, which was developed in conjunction with several financial partners.
   a. In Q3 2019, building toward a full implementation of a private blockchain to handle the transition of credit derivatives to a blockchain, the DTCC published a white paper outlining governance considerations for financial enterprises seeking to implement a private blockchain. The white paper itself is available here.

4. JPM Morgan, the sixth largest bank by assets in the world, has added zero-knowledge proof functionality, a partnership with Microsoft, and signed up over 300 banks to be a part of its Interbank Information Network, running on the private Quorum blockchain developed by the firm.

5. Led by UBS, a consortium of 14 firms have developed a platform, Finality International, to launch a blockchain-based platform to facilitate trade settlements between institutions.

At the same time, however, organizations and practitioners seeking to implement an enterprise blockchain-based solution must also take the following headwinds into account:

1. Customer data and information are both potentially the most valuable asset organizations may have, particularly in the financial services space, but also a virtual treasure of information for hackers and other organizations seeking to extract said data for nefarious purposes.
   a. Because customer and consumer information is so valuable to organizations in virtually every sector, this raises the stakes for how management professionals treat, store, and manage information. While no technology solution, be it blockchain or some other security-driven database management platform, is immune from failure, enterprise blockchain does seem to offer a possible solution. Encryption and security lie at the core of any blockchain platform, which can help to mitigate the embedded risk in changing how data is handled and transferred between stakeholders.

2. Blockchain, even the enterprises that have currently implemented blockchain-based solutions and options, still represents an emerging and nascent technology. The original bitcoin blockchain, which subsequently launched the entire ecosystem, only entered the marketplace beginning in 2009.
   a. From an implementation perspective, the very early stages of enterprise blockchain development highlight risks and potential headwinds for entities seeking to do so. In addition to the lack of understanding and general awareness from an employee basis, this nascent stage also increases the risk from a liability, insurance, and governance perspective. Put simply, many of the products and support services that accompany database management tools simply do not exist for mainstream utilization at this stage. Although, as noted above, security is at the center of blockchain, the dearth of support services and products does pose a substantive risk.
3. Building on the second point, as the technology itself continues to develop and mature, the regulatory landscape, both in the United States and on a global basis, will continue to evolve.

   a. Especially in the financial services space, the differentiation between regulatory bodies and jurisdictions can have a dramatic impact on how data is treated, regulated, and stored. In addition to impacting who has access to this data, the penalties and implications of data mismanagement will differ depending on where these violations occur. Due to the fact that blockchain by its nature encourages storing and transmission of information, it remains a fiduciary duty of all associated management professionals to remain aware of how different legal frameworks can either accelerate or impede broader adoption.

Financial Services Implications

Analyzing the implications of blockchain for the financial services industry requires an acknowledgment of the origination of the idea itself. The core—and some adopters would say purpose—of the blockchain idea was to disrupt and remove financial intermediaries from business transactions and record keeping. Taking this into account, the development of enterprise blockchain applications by many of the largest financial institutions in the world does not seem like a surprise or shock. Early adopters and enthusiasts may be disappointed that enterprise blockchain does represent a shift toward centralization, but this should not be perceived as a radical departure or change. Rather, it seems to be a logical response to the existential threat posed by blockchain to both operational success and profitability of major financial institutions. Drilling down specifically into what types of transactions may be appropriate for blockchain augmentation and improvement, several examples do come to mind:

1. Interbank settlements
2. Cross-border transactions
3. Settlement of trades and bond issuances
4. Letters of credit

All of the above-listed classes of transactions have several core characteristics in common that appear to make them prime candidates for blockchain augmentation. First, all involve multiple stakeholder groups that may operate inside or outside of the primary organization, complicating matters from a data transparency and standardization perspective. This is especially important if different jurisdictions and regulators have different laws and regulations connected to how customer and financial data should be handled. Second, due to these multiple layers of intermediaries and third parties, the complexity and cost of doing business in these situations can rapidly increase, eroding both customer satisfaction and margins for those parties involved. In a market environment already facing margin compression and new entrants, adding these incremental costs only contribute to this margin pressure. Third, but connected to the previous two points, is the interoperability internal control considerations that must be coordinated between these various entities. On top of traditional interoperability issues, the ones raised by blockchain implementation raise additional governance, cybersecurity, and compliance considerations for all involved practitioners. Let's take a look at how the implementation of an enterprise solution might be able to assist in a quantitative manner with current pain points and stumbling blocks associated around current processes.

This is simply one example—albeit a high profile one—of how blockchain is already being implemented by some of the largest financial institutions on the planet. In addition to the financial implications of this implementation, it also demonstrates the implied value of this technology. While the specifics will vary
from organization to organization, there are several pain points in every financial transaction and process that involves different organizations. First, if funds or trades are processed or sent across national lines, there is virtually always a need for a correspondent banking relationship, as indicated by the utilization of a nostro/vostro account situation. In essence, what this means is that every bank or financial institution wishing to conduct business with other institutions, especially those located overseas, must allocate capital and technology resources to address the currency, regulatory, and technical issues that currently can hamstring operational efficiency. These resources are necessary because of the time it takes for banks, payment processors, and other financial counterparties to coordinate, communicate, and verify the transactions themselves.

Linking back to the point listed above, it is especially important from an enterprise perspective to understand that the more counterparties, review processes, and manual verifications that are involved in a transaction or process provide opportunities for errors, omissions, or unethical actors to take advantage of breaches in the security protocols in related systems. An enterprise model of blockchain, be it constructed as a public-permissioned, private, or consortium model, can assist in addressing a paradox emerging in the blockchain space. As different organizations are implementing blockchains internally, how can these models be linked together to generate efficiencies between the firms seeking to do business together? Every organization is different and will have specific criteria that take priority within the firm, but it is going to be important for organizations and practitioners to make every effort to establish consistency and interoperability across blockchain options.

Drilling down into some of the specific benefits connected to further blockchain adoption, there are several that are already being realized and demonstrated by adoption across the financial services sector. First, and perhaps the benefit that has been recognized in the most obvious manner, is the reduced need for corresponding banking relationships if a common blockchain platform has been established. If a group of financial services organizations coordinates and operates a common blockchain platform, this—by the nature of the technology itself—means that data is being shared on a nearly continuous basis. Because this information is shared so efficiently and relatively quickly between partner organizations, this also means that confirmations and settlements can occur in a more time-efficient manner. Second, and particularly important given the recent string of fines and violations connected to banking and other financial services institutions, the implementation of blockchain increases the transparency and traceability of information. While not a surefire solution or panacea to the problems connected to money laundering—and raising new questions as they relate to KYC and AML regulations, blockchain does seem to offer at least a partial solution. Since transactional data is time-stamped and shared between network members, this creates a virtually ready-made audit trail that can be used by both internal and external participants. In terms of both improving the financial and operational audits that already exist, this also demonstrates the potential—and reality—of blockchain to assist in improving enforcement of anti-laundering legislation.

**Financial Services—Risks and Opportunities**

Some of the core benefits of an enterprise blockchain integration include the potential improved speed with which transactions and other financial information can be processed, the potentially lower costs for doing so between different financial institutions, and the traceability of information in a nearly continuous manner. Building on the importance of traceability in the financial system, the benefits that are able to be delivered include improving current audit and attestation practices, as well as reinforcing the trust and transparency of the financial system. In an era of increased global instability, including both economic and geopolitical uncertainty, increased confidence in the financial system is paramount. Circling back to the numerous fines and citations brought against global financial institutions for money laundering and being
complicit in other unethical actions, the traceability of data stored and transmitted on a blockchain-based platform represents a definitive business benefit.

Particularly for e-commerce (which is global by nature), cross border payments, and the settling of various financial transactions, the benefits and upsides of an enterprise blockchain solution are relatively clear. These benefits and opportunities, however, also come with a certain degree of risk and exposure, especially as it pertains to the compliance and reporting aspect of the information stored on a blockchain platform. Drilling down specifically, a few of these risks include, but are not limited to the following:

1. Maintaining data integrity and consistency as blockchain platforms become integrated and also compete for a dominant market position.

2. Avoiding the possibility that one single enterprise blockchain option, such as a Quorum model, which is in use at JP Morgan and was adopted as the officially supported option in the Microsoft Azure cloud in 2019, assume an unassailable dominant position.

3. Navigating the regulatory uncertainty that continues to surround the blockchain space, especially from a compliance and cybersecurity perspective, not to mention the issues that arise when coins, tokens, or other cryptocurrencies are added to the conversation.

Building on the third point listed above, perhaps the biggest single risk from an implementation point of view is the uncertainty and ambiguity that continues to dominate the conversation from a risk and liability perspective. As increasing amounts of personally identifiable information, which includes financial data and transactions, are stored and transmitted via blockchain options, it is logical to point out a risk that may arise over time. Not every blockchain is constructed using the same encryption or security protocols, so ensuring that these protocols are both understood and appropriately implemented is a fiduciary responsibility of all motivated stakeholders.

**Conclusion**

Regardless of which specific blockchain project or implementation is examined, it does appear logical to conclude that the pace of investment and integration is set to continue accelerating moving forward. Even given the regulatory pushback and scrutiny that continues to represent a headwind toward broader-based adoption, the use cases and applications of blockchain for financial services continue to become readily evident. Focuses of specific projects and implementation can focus on reducing costs, increasing the transparency related to the transfer of funds, or the development of different cryptoassets—but no matter the specific end goal of the project, the underlying themes are the same. Increasing the security linked to financial transactions, enabling greater access to financial services on a global basis, and assisting with the maturation of the conversation linked to cryptoassets all represent roles that financial institutions can assist with moving forward. Leveraging the embedded expertise of financial institutions with handling consumer and financial information means that—far from being disrupted—financial institutions across the world have an important role to play in the blockchain ecosystem going forward. While it is impossible to forecast how exactly blockchain technology will develop over time, the fact remains that the future seems dynamic and promising for financial services organizations.
**Dr. Sean Stein Smith** is an assistant professor of accounting in the Department of Economics and Business at Lehman College (CUNY). Sean also serves on the Advisory Board of the Wall Street Blockchain Alliance, where he leads the Accounting Working Group, and serves as the chairperson of the New Jersey Society of CPAs Emerging Technology Interest Group. Sean served as an E.C. Harwood Visiting Research Fellow at the American Institute for Economic Research during 2019 and has had books published, or that are in the publication process, at Taylor and Francis, Springer, and Palgrave-MacMillan. Sean has been named one of the “Top 100 Most Influential People in Accounting” by Accounting Today.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, taxexempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2019 by the Center for Strategic and International Studies. All rights reserved.