DEPTH. FOCUS. SERVICE.

MERCATOR
ADVISORY GROUP

ARE BLOCKCHAIN SOLUTIONS READY?

THREE BLOCKCHAIN SOLUTIONS PUT TO THE TEST

A Mercator Advisory Group Research Brief Sponsored by CO-OP Financial Services and TMG

October 2016

CONTENTS

Introduction

The emergence of blockchain and immutable ledger technologies generated much interest and excitement in the financial services industry. The excitement has led to discussions at every level of business operations, including CEO and Board discussions, primarily because these technologies are purported to be the infrastructure that will disrupt the financial services industry. In light of the high visibility of this nascent technology, CO-OP Financial Services and TMG commissioned Mercator Advisory Group to establish a **Strategic Framework for Evaluating Blockchain Solutions** to determine if such solutions deliver a compelling use case and if they are ready for deployment in the highly regulated financial services market. This effort has focused on evaluating solutions that utilize blockchain technology and not just blockchain technology platforms, such as Ethereum, that are designed to support multiple solutions. This approach was necessary so ascertain how effectively a given blockchain solution addresses specific market needs, such as the security, performance, and regulatory requirements associated with the specific use case implemented. This approach does not address internal pilot tests and research efforts that may be underway or gauge how quickly they might bear fruit, but it does provide a clear snapshot of a blockchain solution suggesting how quickly it may be available as an off-the-shelf product.

Recently, application runtime capability has been layered on top of the blockchain to enable the distributed execution of contracts between participants using a computer protocol called a “Smart Contract.” In concept, once participants agree to such a contract, it is executed by the distributed blockchain, thus eliminating contractual disputes. The most visible solution today is Solidity, a Smart Contract solution built on top of the Ethereum blockchain platform. However, Smart Contracts were not evaluated for the Strategic Framework for Evaluating Blockchain Solutions presented in this research brief for two primary reasons. First, no solutions relevant to financial institutions have been implemented as yet utilizing Smart Contracts technology. Second, a Smart Contract solution called the DAO (for Decentralized Autonomous Organization) was severely hacked recently, resulting in the theft of $50 million worth of the virtual currency called Ether. For these reasons, Mercator Advisory Group determined that it is much too early to consider Smart Contracts ready for testing, much less deployment, in financial services.

The research presented here focuses entirely on evaluating how prepared blockchain solutions are to address highly regulated aspects of the financial services market. It does not apply to implementations utilized internally, in pilots, or in unregulated or lightly regulated markets. Several large banks have announced with much fanfare that they have implemented internal pilots or interbank pilots that utilize blockchain technology. These pilots help advance the development of the technology to address specific use cases important to a given institution, and they help the institution better understand the current limitations of the technology, identify security and regulatory issues associated with specific use cases, and build blockchain expertise within the organization. In addition, announcing a blockchain pilot delivers a strong message of technological leadership to the market. This leadership position, however, comes at great cost and risk since the return on investment is unknowable. For smaller institutions interested in building internal expertise, several low-cost blockchain cloud solutions are available that can be applied to internal pilots at lower cost and risk. However Mercator Advisory Group suggests that given the current state of blockchain technology, those investment dollars may be better spent on developing expertise and solutions that have a shorter implementation timeframe, such as machine learning and biometric authentication technologies.

It is impossible to perform an evaluation of solutions that utilize blockchain technology without recognizing the unique advantages this technology delivers as well as the limitations currently associated with delivering those unique advantages. For example, blockchains maintain a shared perspective of transactions across untrusted participants using a trust algorithm. But implementing this trust algorithm typically greatly reduces overall transactional throughput. This reduction is driven by the need to propagate a shared perspective of each transaction across a network of systems across networks of differing speeds, all while maintaining assurances that no one participant is using the delay in transaction delivery to insert false or duplicate transactions. This is just one relatively simple example of the trade-offs that are necessary in order to deliver the benefits associated with blockchain technology, and there are more. As a result, when considering the use of blockchain technology it is very important to make sure the solution ***requires*** the unique benefits the blockchain delivers. As an example, it makes no sense to implement a blockchain as a replacement to an existing centralized database. An application that doesn’t require a distributed database but does need high transactional throughput and the ability to change the stored data structure will be better implemented on a traditional database. This was perhaps best illustrated during the evaluation of the Guardtime solution, which eliminated an important technology central to blockchain operations to assure maximum transactional throughput, which was a wise decision to make sure the solution can solve the problem it was designed for.

Mercator Advisory Group worked with CO-OP Financial Services and TMG to identify three blockchain solutions to evaluate. The three solutions selected are:

- **Evernym**, a self-sovereign identity (SSI) solution that enables consumers to collect personal information from multiple corporate and government sources and then share the collected information or simply validate the truth contained in that information to any requester.

- **Guardtime**, a product that interfaces to existing internal data sources, such as databases and computer and network log files, and creates an immutable history of those data sources utilizing blockchain technologies. If hacked, this immutable history will enable detection and recognition of the hack and the undesired changes to internal data structures, validating the integrity of system files, applications, and databases.

- **Ripple**, a solution from Ripple Labs that uses blockchain technology to settle cross-currency payments efficiently by directly connecting banks.

This research briefly describes blockchain technology, identifies software management and maintenance issues associated with deployment of a blockchain, provides a brief explanation of the criteria used to perform the evaluation, reviews the findings for the three products evaluated, provides key findings regarding the status of out-of-the-box solutions built on blockchain technology, and provides Mercator Advisory Group's recommended approach for monitoring blockchain solutions to assure resources are assigned appropriately—that is to say, not too early in the development cycle but not so late that you miss a potential first-mover advantage.

Note that because of the nascent stage of blockchain solutions, this project did not evaluate a range of issues associated with cost of operations, service levels, and other critical areas that are considered standard in a typical request for proposal, or RFP. With regard to those areas, it can be safely assumed that there will be direct and indirect costs associated with operating a blockchain solution that have yet to be established or even fully understood. If the blockchain is managed in a cloud configuration, the cloud business model suggests a costing model that will be similar to that of other cloud-based solutions. Regardless, software must be managed and updated, and so there will be costs associated with this function that will need to be paid for by participants in the value chain.

Less obvious, but also important in evaluating a blockchain solution although not addressed in the present evaluation, are the potential costs associated with maintaining and reconciling two sets of books. If the blockchain solution is the single source of history, then there is only one set of books and no additional effort is required. If, instead, the blockchain is integrated to internal systems that maintain a separate transactional history that includes data not represented on the blockchain, such as partner fees, then reconciliation will likely be necessary. This is often a trade-off associated with the use case, in that maintaining all aspects within the blockchain eliminates reconciliation efforts but also makes it difficult to extend the solution to support new data elements. As blockchain technology exists today, adding new data elements requires all participants to agree to the modifications and to a deployment plan for rolling out the new data structure.

It should also be noted that these evaluation results are specific to the blockchain technology and infrastructure that existed during the evaluation effort. Since both technology and regulations change, the results of this evaluation may become less relevant as technology and regulations evolve over time.

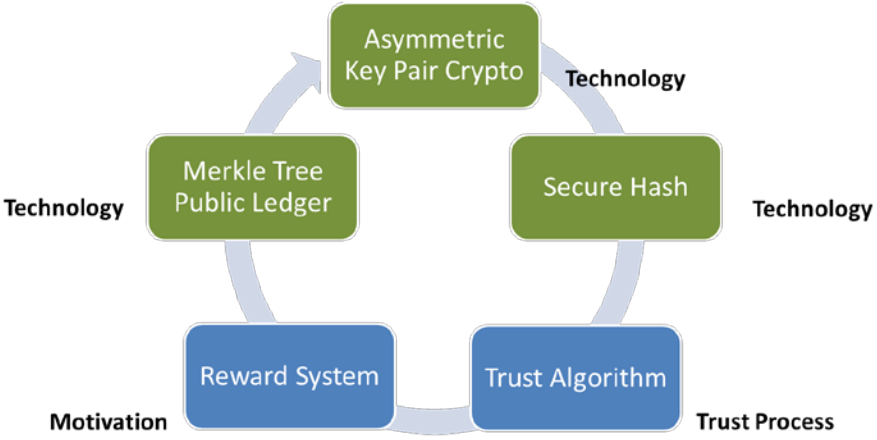
The Operational Components of a Blockchain

It is important that there be agreement regarding what constitutes a blockchain prior to implementing an evaluation of blockchain solutions, but achieving that agreement is not as straightforward as might be assumed. For example, the applications Mercator evaluated for this project each included significantly different technical implementations of a blockchain. One had eliminated a key component. Another had established multiple blockchain implementations within an architectural framework in an attempt to overcome the throughput limitations inherent in the operation of a blockchain.

To clarify, therefore, we begin with Mercator Advisory Group's technical review of blockchain technology, followed by a description of how some implementations utilize the term blockchain without providing a full solution.

Five key operational components form the foundation of the Bitcoin blockchain as identified in the original Satoshi Nakamoto white paper. These five components, illustrated in Figure 1, are tightly coupled within the Bitcoin ecosystem, which makes the extraction of any one of them impossible without having a large negative effect on the overall operation of the blockchain, as will be described later. Many different approaches are being taken today to liberate the blockchain from the constraints inherent to this Bitcoin implementation, but it should be recognized that any alternative approach must address all aspects if it is to deliver similar operational benefits:

Figure 1: The Operational Components of the Bitcoin Blockchain



Source: Mercator Advisory Group

Asymmetric Key Pair Crypto

The technology known as asymmetric key pair crypto is widely trusted and deployed today in many different implementations, including online security solutions deployed to protect Internet traffic. It consists of private keys tightly coupled to public keys. In the blockchain implementation, transactions are encoded with a private key and can only be decrypted using the associated public key. In Bitcoin, the owner of a coin holds the private key and encrypts a spend message using that key. On receiving a coin, the recipient can validate the sender owns the coin by decoding the message using the public key. When a public key decodes the message properly, that decoding is assurance that the message was sent by the private key associated with that virtual coin. In non-Bitcoin solutions, developers often make significant changes to the way the asymmetric key pair crypto is implemented to address use cases beyond cryptocurrencies. It is expected that this cryptography may be compromised in 20 to 30 years as technology evolves, so having a method of re-encryption is prudent if data must be secure for a longer time.

Secure Hash

The National Institute of Standards and Technology (NIST) algorithm (SHA-256) known as Secure Hash is used to generate a unique 256-bit hash of any data which is consistent every time it is executed against the same dataset. In the Bitcoin blockchain, a hash is created for every set of transactions that have been approved and that hash also includes the hash created for the previous set of transactions. The combination of all accepted transactions and the linking of all past transaction sets to the current transaction set utilizing linked hashes creates an immutable ledger because if even one bit of any past transaction set is modified then a re-hash of that transaction set will not equal the original hash, which makes the corruption visible and easily detected. Note that this algorithm is often called a one-way hash because the original data cannot be re-created by evaluating the output of the hash function.

Trust Algorithm

Preventing a double spend of cryptocurrency was a critical component of Bitcoin. It was solved by Satoshi Nakamoto with a Proof of Work algorithm that is tightly coupled to a Reward System that encouraged honesty (as discussed next). Space is insufficient here to describe workings of the Bitcoin Proof of Work algorithm, but it is important to understand that this is the algorithm that bitcoin miners perform in an effort to be rewarded with bitcoin currency. The algorithm requires significant computing power to solve and is designed to take on average 10 minutes to solve. As computers become faster, the algorithm is altered to increase the degree of difficulty so that it always takes 10 minutes to solve. This specific trust algorithm provides mathematical certainty that no fake transaction can be inserted into the Bitcoin blockchain unless more than 51 percent of all nodes performing the algorithm are compromised. The benefit of this algorithm is that it is mathematically certain, but the downside is that it greatly reduces transactional throughput. Significant effort is being made to establish a similarly mathematically certain level of trust while greatly increasing the speed with which this trust can be instantiated through a new model called Proof of Stake. The present research does not include a study of how effective these new algorithms are, but Mercator expects that a Nobel Prize will be awarded to anyone that can create a trust model as secure as Bitcoin’s but with substantially greater throughput.

Reward System

Because Bitcoin miners are rewarded with bitcoin (either created by the Bitcoin system or as per-transaction fees), each miner has a personal interest in not undermining the intrinsic value of bitcoin currency, which would fall precipitously if it became known that miners were cheating. In the event that 51 percent of all bitcoin nodes ever comes under the control of a single entity, that entity will face a conundrum. While fraudulent spending is possible, that fraud will quickly be discovered (see Secure Hash section above, which describes the immutable ledger), causing the value of bitcoin to drop precipitously and thereby eliminating future income for the fraudsters. As a result, it is likely that potential fraudsters will simply utilize their greater computing power to reap more bitcoin without conducting fraudulent transactions.

Merkle Tree and Public Ledger

In the earlier description of the Secure Hash, it is evident that keeping every transaction set for all time would create a database so large that would eventually become impossible to manage. The Merkle Tree algorithm recognizes when data is no longer active and enables those transactions to be deleted. As an example, if all the value of a bitcoin has been sent to another user, then the details of the past transactions can be deleted as long as the hash chain across all transaction sets remains. This is a critical technology for the ongoing maintenance and operation of Bitcoin, and any derivative versions of the Bitcoin blockchain must consider how much data is stored and when it can be deleted.

Evolving the Blockchain

Brilliant people at universities and large corporations may well accomplish the goal of a blockchain solution that not only equals or improves on the current algorithms implemented in Bitcoin but also utilizes less power and validates and distributes transactions faster than existing distributed databases, but this is far from guaranteed. The current efforts to simplify Bitcoin have primarily hinged on altering the Bitcoin Trust Algorithm and Reward System by arguing that the Bitcoin implementation is only needed because it operates in an untrusted environment—that is, anybody can be a Bitcoin miner, even potential criminals. New, faster approaches assume only trusted entities will be allowed as miners, a condition typically termed a “Permissioned Blockchain.” Note, however, that even in the existing banking system, trusted entities can be involved in criminal behavior, as was demonstated in the Libor incident.

The evaluation matrix does not include a metric to measure the validity of any particular trust algorithm because that is not a function that can be easily or reliably measured. Some algorithms, such as Evernym’s, are so complex that a mathematical proof is unlikely to be possible, or at least certainly not by us. But even if math identifies trust has been achieved for all but a few situations this does not imply that implementation or operational issues might not cause the system to fail.

> What can be evaluated is how well a particular use case leverages the distributed ledger, accommodates the longer transaction approval cycle dictated by the trust algorithm, and accommodates the file structure of the ledger, aligns with the idiosyncrasies of the Asymmetric Key Pair privacy and security model, and addresses data residency issues when operational nodes are distributed across multiple countries.

These technical topics are discussed later, but first we evaluate deployment issues that are external to blockchain technology.

Attributes Required for a Technology Solution to Be Called a Blockchain

Following is Mercator Advisory Group's definition of a blockchain:

> **A blockchain operates across distributed nodes, located in multiple locations, connected by the Internet while assuring that a single perspective of accepted transactions is maintained by participating nodes even as each participating node remains semi-autonomous (capable of continued operation even as other nodes fail). This implies a robust trust algorithm that offers resilience to denial of service attacks.**

Defining blockchain this way eliminates the Guardtime solution as a true blockchain. Guardtime provides a very important service that makes hacking, and any damage caused by hackers, visible and traceable using an immutable ledger. Guardtime establishes a hash of database and system files resident on a company's servers and stores the hash in an immutable ledger. To deliver the performance required in order to keep up with file changes made across multiple systems, and because it operates within a trusted environment, Guardtime decided to eliminate the trust algorithm, and Mercator agrees with this decision. However, according to the definition of a blockchain above, Guardtime is an immutable ledger but is not a blockchain implementation.

Note that the definition above does not specify or clarify how the capabilities are implemented, how robustly the implementation solves for collusion, or exactly what attack vectors the technology is capable of resisting. In particular, Mercator finds the argument that substantial protection against collusion is not required when the blockchain is implemented by trusted nodes in a permissioned environment is totally dependent on the use case, again referencing the Libor incident.

Identifying External Issues That Require Evaluation

All software solutions, the blockchain included, are human endeavors that operate within a human-designed legal and societal construct. As a result, we humans are the major hurdle preventing blockchain adoption. It would be unreasonable to assume that no errors will be made, no solutions will malfunction, and no operations will face criminal activities against the technology or the developers, or that blockchain solutions do not need to operate within the laws of the land created to protect our societies.

Many in the blockchain community argue, as IBM's Jerry Cuomo did in a May 2016 blog[i], that our government must change laws to recognize the new trust model that the blockchain purports to create so that blockchain solutions can more quickly deliver competitive advantages to the United States. Perhaps some laws will be changed or new ones enacted, but those changes will take longer to occur than most organizations care to wait, and mistakes that occur along the way, such as the Decentralized Autonomous Organization (DAO) fiasco,[ii] will almost certainly slow the government's willingness to take a leap of faith. This suggests that it will take significant time for laws to be adapted to blockchain.

By nature, human beings seem to find it convenient to hold someone or some entity accountable when things go wrong. As such, it is hard to imagine that laws will be passed that eliminate legal accountability. It is more likely that early adoption of blockchain technologies will be implemented under existing laws, utilizing existing businesses or consortiums, which is the case for all three solutions evaluated here. This is the assumption made in the creation of the Strategic Framework for Evaluating Blockchain Solutions, outlined below. These external issues fall into two categories: those associated with existing regulations, and those associated with a need to provide settlement when a transaction is conducting any form of trade or value transfer.

The Strategic Framework for Evaluating Blockchain Solutions

Mercator Advisory Group's matrix evaluates 39 distinct functions in five key areas associated with deploying a blockchain solution, including both technology issues and questions regarding specific regulatory issues and several settlement questions. These are summarized below.

Alignment with the Unique Capabilities a Blockchain Delivers

Blockchain implements an immutable ledger that maintains a shared view of time-ordered transactions across multiple independently operated nodes that are managed by some coordinating entity.

If these capabilities are not required for a use case, then perhaps other technologies will prove more appropriate for deployment.

Ability to Execute Within the Blockchain's Unique Transactional Structure

The blockchain ledger structure has limited flexibility as compared to other data distribution technologies, such as cloud computing and traditional distributed databases. This area of the framework evaluates the application's needs for complex data structures that are not easily implemented with existing blockchain technologies.

If the use case requires sophisticated transactional capabilities, then other technologies may prove more appropriate for deployment.

Ability to Execute Within the Blockchain's Unique Security Model

Blockchains implement privacy and immutability utilizing public/private key pairs and a trust algorithm (proof of work, or PoW, proof of stake, or PoS, etc.) that time-orders transactions and propagates that order to all nodes. This approach makes complex permissions difficult, if not impossible, to implement. Also, transaction availability across the network may be difficult or impossible to predict.

If the use case requires rapid sharing of data or requires complex controls determining which entities have read access or write access to the transactions or even to just specific parts of the transaction, then other technologies may prove more appropriate for deployment.

Evaluating External Regulatory, Data Ownership, and Residency Requirements

Blockchains are deployed across multiple nodes and the trust algorithm and the data contained in the ledger may be made available to any entity interested in executing a node, in any geography, and that entity may be a participant or nonparticipant in the ledger use case, and the entity may or may not receive compensation.

The structure controlling how the proof-of-work algorithm is deployed will have a major impact on how regulatory agencies perceive risk and compliance to existing regulations.

Evaluating Settlement Requirements

Blockchains utilize a trust algorithm that requires time to identify and propagate the shared perspective related to the transactions that have been accepted and the specific ordering of those transactions. If the blockchain includes its own currency or is linked to an external money movement, the money movement should not start, nor should it be finalized, until the transactions are properly cemented in the ledger.

When the currency isn't native to the blockchain, external exchanges are often used for settlement between participants. These exchanges are executed outside of the trust algorithm and have consistently been shown to be extremely risky. Understanding the systemic and transactional risk associated with the settlement function is of course critical.

The Three Blockchain / Ledger Solutions Selected for Evaluation

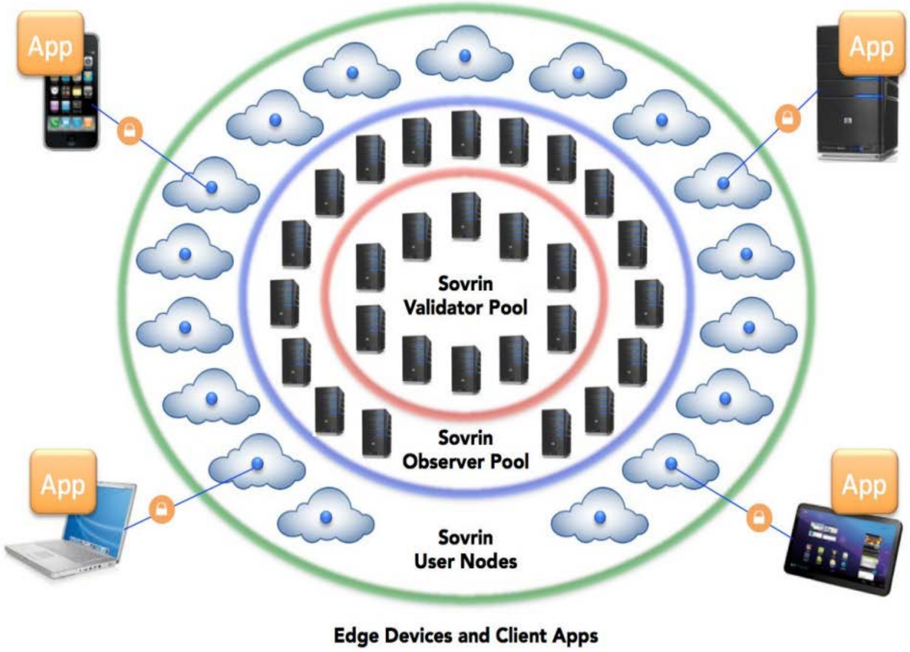
Mercator evaluated three use cases against the evaluation matrix, two selected by CO-OP Financial Services and TMG and the third selected by Mercator. The three use cases included an identity solution, an international bank to bank remittance solution, and at Mercator's choice, a security solution. Below are descriptions of each solution, our observations regarding the evaluation process and our conclusion regarding how appropriate the technical solution is to its use case.

Evernym

Evernym designed and is currently implementing a blockchain that will deploy nodes in a multi-tier, trusted distributed infrastructure. Financial institutions have been looking for a mechanism through which the identity information they hold regarding customers might be leveraged more broadly and other external sources of identity might become usable for their own internal processes.

This mechanism is the goal of Evernym in the Sovrin Architecture, which is illustrated in Figure 2.

Figure 2: The Sovrin Architecture Uses Multiple Ledgers in a Hierarchical Relationship



Source: Evernym, Sovrin Technical Overview PDF

The Evernym design utilizes a multi-tier blockchain structure designed to mitigate performance issues associated with both reads and writes on the ledger as well as to support governance issues. To make the solution broadly available, Evernym announced on September 29, 2016 it was donating the intellectual property for the underlying distributed identity ledger technology to an international nonprofit organization called the Sovrin Foundation, which will be responsible for the worldwide governance of the Sovrin Network.

The Sovrin Foundation initially consists of a Board of Trustees with a minimum of nine members and a Technical Governance Board that reports to the Board of Trustees. This structure is designed to deliver governance and accountability across multiple geographies and will control the software development and management functions to meet those goals. While a primary purpose of this design is to meet regulatory requirements, it is unclear to Mercator how this will be possible given potentially conflicting government regulations on privacy and data residency.

While certain aspects of the identity solution use case are well aligned with a blockchain implementation, such as providing user with control over their own data, other aspects suggest the solution could be implemented faster and easier utilizing cloud technology rather than a blockchain. The architecture needed to achieve performance for a worldwide solution, with every node linked and updated, is significantly complex and these distributed nodes will create challenges when attempting to meet every country’s regulatory construct with all nodes operating the same software and data being distributed everywhere.

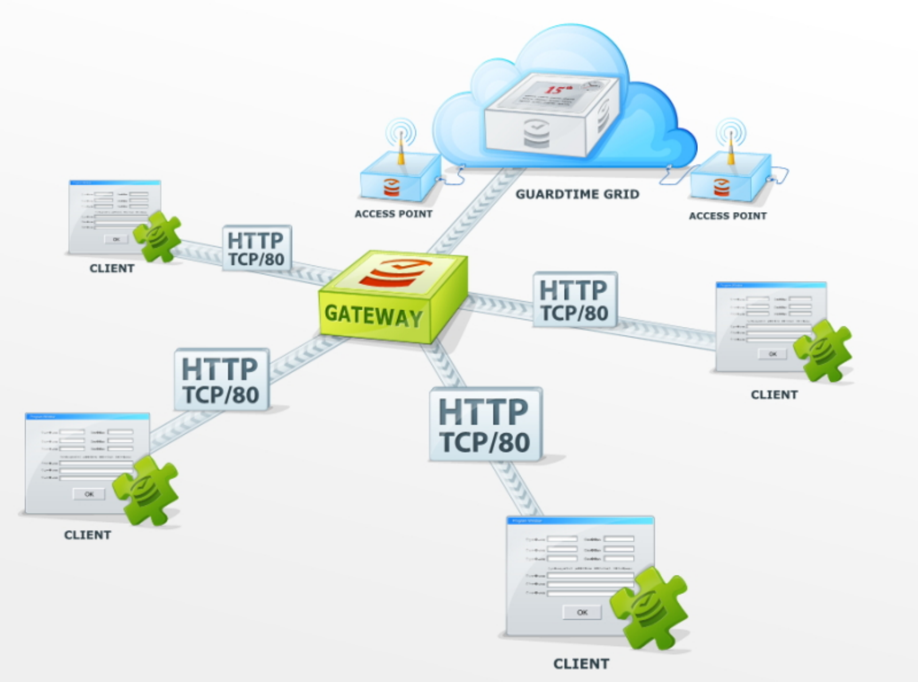
In light of Evernym's decision to create an international charitable organization to control, manage, and operate the solution, it appears likely that this organization will discover that it would have been easier to meet international regulations by having traditional cloud services located in each geography with data remaining local, and to have those services connected by a gateway when data needs to move between regions. This is similar to the architecture of Netflix, albeit on steroids.

The Evernym use case is groundbreaking. Enabling validators to provide consumers their own data to confirm their identity without divulging facts is a beautiful idea that stretches our imagination. Putting such a groundbreaking concept onto a modified blockchain may delay the release of the solution for years.

Guardtime

Guardtime is a software security company founded in Amsterdam shortly after the April 2007 Russian cyberattack on the Estonian parliament, banks, ministries, newspapers and broadcasters. The product is used to detect hacking and to identify the data objects that were modified by the hackers.

Figure 3: Guardtime Collects and Digitally Stamps Data from a Range of Sources



Source: Guardtime

Guardtime monitors files and databases resident on external computers or any other digitized object and creates a linked hash associated with the original and every modification. The linked hash creates an immutable ledger that is stored externally which is used to recognize if data has been tampered with. Because a hash is relatively simple to calculate, Guardtime can monitor very large sets of data that are modified frequently. Because the hash is not based on asymmetric key pair cryptography and is impossible to reverse engineer, Guardtime is both very secure and resistant to the quantum computing hack that puts PKI solutions at risk over the next 20 years.

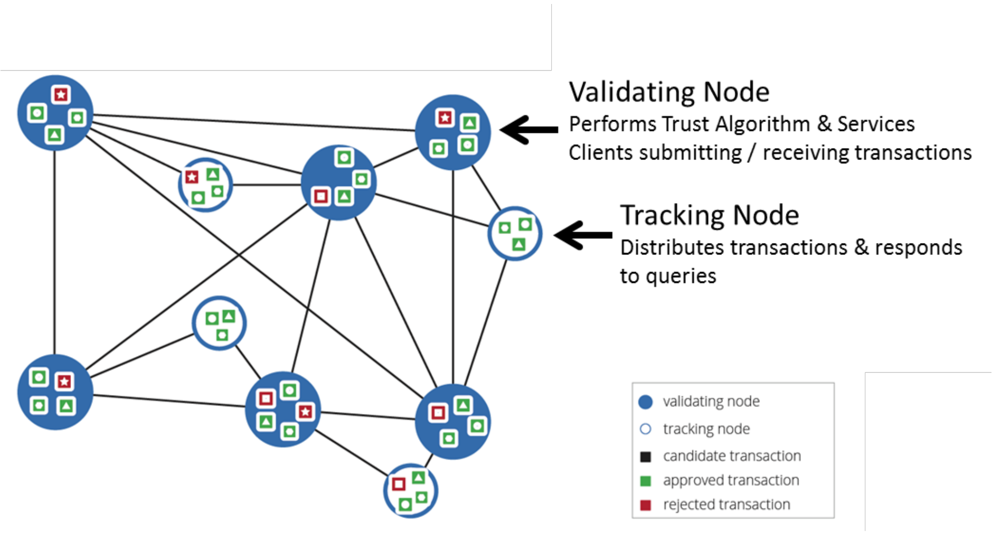
Guardtime, created to secure Lithuania's government digital assets, has also been adopted by China, the Philippines, and in the United States, where it signed a licensing agreement with U.S. military technology company MTSI to deliver Keyless Signature Infrastructure (KSI™) Insider Threat Services to the U.S. defense and intelligence communities.

While Guardtime describes its technology as using blockchain technology, this definition is a stretch since of the five components that establish a blockchain, Guardtime utilizes only two, the Secure Hash and Merkle Tree, which are combined to create an immutable ledger of external data.

Ripple

Ripple's distributed network, based on blockchain technology, enables banks around the world to directly transact with each other without the need for a central counterparty or correspondent banking relationship. Unlike Evernym, which is developing a complex business structure and architecture to address a perceived use case, Ripple has already pivoted from its original use case of being a remittance product for consumers to one that is designed specifically to address the needs of banks and now has six banks participating and more to be announced shortly. The initial Ripple design incorporated end users, banks, and exchanges in a tightly coupled environment that made all transactions visible. This solution utilized a blockchain construct that is based on the Ripple Consensus Protocol,[iii] which utilizes permissioned nodes in the fashion identified in Figure 4.

Figure 4: Ripple Implements a Hierarchy of Nodes to Manage Performance



Source: Mercator Advisory Group based on Ripple Labs information

Ripple Labs discovered the risk associated with directly enabling consumers to move funds internationally in May 2015 when the U.S. Financial Crimes Enforcement Network (FinCEN) issued a civil enforcement action stating that Ripple had "willfully violated several requirements of the Bank Secrecy Act (BSA)" including “failing to implement and maintain an adequate anti-money laundering (AML) program” and fined Ripple $700,000.[iv] Lesson learned.

Today Ripple recognizes the regulatory challenges associated with enabling direct participation of consumers with respect to Know Your Customer requirements and has learned that financial institutions expect to make their transaction history available to regulators but keep it a secret from competitors. As a result, Ripple Labs has recently hired experts from SWIFT, brought in legal counsel, and introduced new protocols and services that directly address these and other newly perceived concerns. For example, Ripple has introduced the new Inter Ledger Protocol (ILP), which can be applied to the problem of transferring value between two banks reliably, securely, and while limiting visibility to the transaction. Ripple has also introduced the Ripple Connector, which connects core banking systems to the Ripple network.

In short, Ripple is adjusting its technology, focus, and organizational structure to meet the needs of banks with respect to bank-to-bank international money transfers. Ripple performed well in Mercator’s Strategic Framework for Evaluating Blockchain Solutions for its alignment with the principles of the blockchain, and in the Transactional and Security sections of the Framework, but its results for the Regulatory section remain a sticking point and Ripple will need more time to make all of the changes required to address these regulatory challenges. The company states that an announcement to address this very issue is imminent.

Key Findings

The fact remains that all blockchain trust algorithms evaluated still have a basic trade-off. These algorithms deliver a shared perspective on approved transactions across multiple nodes, but they do so by sacrificing performance and flexibility of the structure of the transaction. Desired but yet to be attained is a trust algorithm that delivers both trust and performance. The Ripple solution requires roughly 5 to 10 seconds to confirm transactions, far faster than Bitcoin, but even that applies an upper limit to the total number of transactions the solution can reliably support. Changing this structure is not easily done because of the distributed nature of the solution.

This trade-off is the reason Mercator’s the Strategic Framework for Evaluating Blockchain Solutions specifically determines if a given use case actually demands distributed nodes that must collectively approve transactions. If it doesn’t, then implementing the solution on a blockchain is accepting the negative aspects of a blockchain for no reason other than to garner market awareness by claiming to have a blockchain solution. Perhaps Guardtime has done it right, as it enjoys the blockchain bump without suffering the negative traits of the trust algorithm—the best of both worlds.

The structure of a transaction within a blockchain is also often constrained, because the fields within the transaction are often validated by the trust algorithm that runs on every node or simply because the transaction format is shared by all participants across all nodes. As a result, the type of transaction being managed on the blockchain and the ease with which that transaction structure can be modified depend very specifically on how the blockchain has been implemented. A common approach, as implemented in Bitcoin, is to create what is called a fork, which typically occurs when nodes are instructed to implement new software. If only some nodes cooperate and others don't, two different instances of the ledger can evolve simultaneously, with the old transactional structure continuing to be used by some constituents and the new structure available for use by others. This brings us again to the problem of defining what is, and what is not, a blockchain.

Shakespeare's Juliet says, "A rose by any other name would smell as sweet" referring to Romeo's lineage. Unfortunately this saying doesn't apply to software in general and certainly doesn't apply to the term 'blockchain'. All three solutions evaluated here claim to be blockchain technology, but Guardtime isn't and Evernym has a version with so much additional technology layered on top that it is hard to recognize where blockchain technology starts and stops. And although Ripple's Ripple Consensus Protocol was indeed a blockchain, the new ICP protocol only utilizes the blockchain as an external reference, instead directly connecting the two banks that wish to execute transactions. To Mercator this sounds a lot like traditional payments infrastructures but with a public ledger instantiating every transaction. It seems that the Ripple ICP protocol could be implemented using traditional technology, as could Guardtime's hashing solution, which stores an immutable history of transactions. This could have been accomplished on an SQL database in the cloud and an appropriate private/public key implementation.

This evaluation clearly highlights the focus that has been placed on technology over operational management. Mercator believes that too many blockchain solutions are being brought to market only because the amazing capabilities associated with the blockchain lures technologists into thinking that it is so powerful the rules and regulations that govern our societies will either be sidestepped entirely or modified to accommodate the next big thing—and perhaps they will, but certainly not quickly! The history of Ripple is likely illustrative.

Ripple development began as early as 2004 and was focused on creating an cryptocurrency alternative to Bitcoin, one that would eliminate a reliance on centralized exchanges, use fewer resources for mining, and process transactions faster. The resulting technology and business entity were incorporated in September 2012 as OpenCoin Inc. (although the OpenCoin protocol retained the name Ripple) and received investments from Andreessen Horowitz, Google Ventures, and IDG Capital Partners.

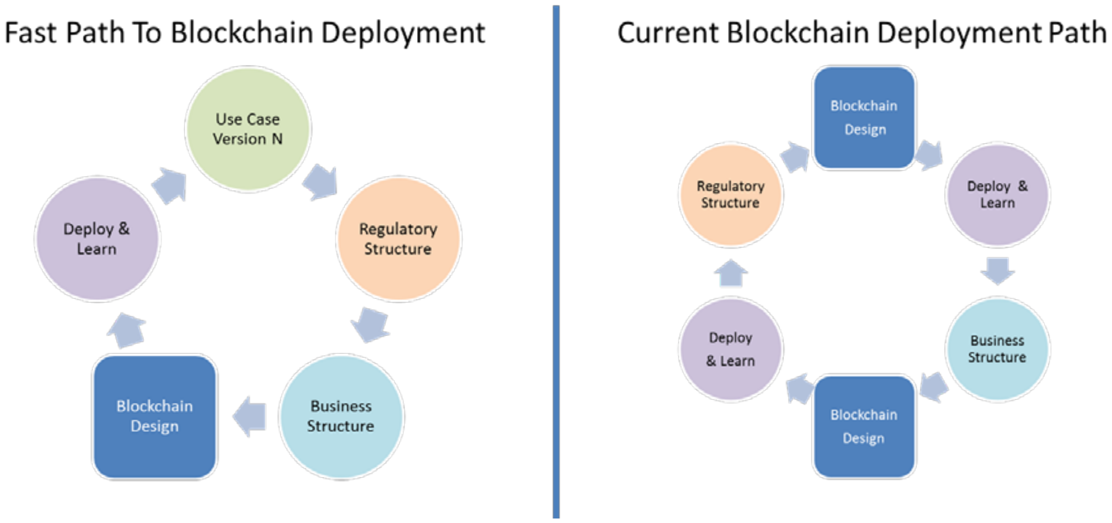
But while OpenCoin technology was faster than Bitcoin, it was not constructed or organized to overcome the regulatory and operational issues that have made most governments and regulators shy away from participation, much less adoption, of Bitcoin. Specifically, OpenCoin enabled consumers to transact without providing identity information, exchanges that could be operated by any entity with sufficient capital, was independent of any geography or country, and established an open ledger by which every participant and transaction could be monitored (pseudo anonymously). To make matters more difficult, this infrastructure was then linked to bitcoin via the Bitcoin Bridge in July 2013. This enabled any OpenCoin user to send a payment in any currency to any bitcoin address—something sure to displease countries serious about efforts to stop terrorist funding.[v]

OpenCoin Inc. changed its name to Ripple Labs Inc.[vi] on September 26, 2013, and by November 2014 was stating that Ripple intended to partner with banks even while replacing correspondent banking into the age of the Internet.[vii] Germany's Fidor Bank was identified as an early adopter that was offering Ripple to its customers.

A blockchain deployed in an unregulated market is primarily a technological and business issue, as is the case for Guardtime. But for blockchain providers focused on banks, credit unions, and payments, the operational and management aspects are more critical than the technology or business value that participants can derive from the solution. In November 2014, Chris Larsen, CEO of Ripple Labs and past co-founder of Prosper Marketplace, identified how past regulatory decisions had not gone in his favor, such as the Securities and Exchange Commission's decision to regulate Prosper, the peer-to-peer loan operator.[ix]

Adjusting technology and organizations to address a new market is not a simple task, and so today Ripple continues to endeavor to be more aligned with the needs of banks and regulators, which is an alignment issue illustrated in Figure 5.

Figure 5: Blockchain Has Been Technology Driven, not the Fastest Path into a Regulated Market



Source: Mercator Advisory Group

The left side of Figure 5 suggests that the fastest path into a regulated market takes into account the regulatory requirements and business case issues before building the blockchain implementation. This is necessary because the blockchain implementation has many design issues that, when implemented incorrectly, greatly slows or entirely prevents the deployment of the solution in a regulated environment. A blockchain company that is willing to wait for the regulatory construct to change will be last to market—if it can survive that long.

The reality that the regulatory and business construct must be addressed first is spawning consortiums at a breakneck speed, but any consortium that expects that it can simply organize itself to deploy existing blockchain technologies is likely to be sadly disappointed. As Mercator's Strategic Framework for Evaluating Blockchain Solutions clearly finds, blockchain technology has many inherent constraints that are incompatible with the needs of a regulated institution. Assuming a consortium can select a specific use case to solve and can staff that effort with experts that cover all of the areas identified on the left side of Figure 5, then the effort is on the right track.

Evernym and Ripple are each in the process of restructuring technically and organizationally into a structure similar to a consortium model to address the business reality that a new business structure is required to address regulated markets.

Although many questions remain, blockchain has spawned an amazing number of new consortiums, most recently including credit unions, the big four accounting agencies, Russian banks, and Japanese banks, and there will almost certainly be more.[viii] Mercator expects many of these efforts will fail or take years before they bring a solution to market. Most will not follow the fast path identified in Figure 5. Many will start with only a vague sense of the specific business problem they intend to address. Nothing confuses a requirements document quite like a standards body or a consortium. If the consortium members do agree on exactly how the solution should operate, and understand how the implementation will address the regulatory structure required (which requires coordination between business people, risk managers, and blockchain architects), then the next problem is how the consortium will be legally and operationally structured. The business and legal issues associated with operating a consortium can be very challenging. Then there is the need to have blockchain architects and software engineers available to design and implement a manageable solution that addresses the business needs and regulatory requirements, and there are very few people qualified to do that job.

Conclusion

Blockchain technology is a breakthrough that delivers a new software capability of instantiating trust and delivering a reliable shared perspective across multiple nodes and participants. But the technology that enables this also constrains performance in ways that are not yet fully recognized or understood. This is in part because the technology is so new, but also because the technology continues to be modified and refined with each implementation in an effort to tune its operation to the purpose at hand.

Mercator Advisory Group is highly doubtful that any one blockchain implementation, such as that under development by Hyperledger, will be capable of supporting all the applications being considered in the regulated payments industry without significant modification to make it suitable to each solution. This suggests that the only viable approach to bringing a blockchain solution to market today is through custom coding that aligns the solution with both the business and regulatory requirements. This type of effort is not for everyone and consortiums that pool resources are likely a good approach, but only if focused on either a single solution or a few solutions that can be proven compatible with the same business model and technology, which has not yet been achieved and which may prove to be impossible.

Mercator Advisory Group's Strategic Framework for Evaluating Blockchain Solutions Evaluation Matrix has proved valuable for drawing out a range of issues in these early days of blockchain deployment but is likely to need updating as the technology evolves. This should not be a problem, however, since today the larger issues are legal and business issues combined with meeting regulatory compliance.

Endnotes

[i] IBM's Jerry Cuomo Blog, May 16, 2016. Accessed 9/3/2016. https://www.ibm.com/blogs/think/2016/05/16/blockchain-securing-the-financial-systems-of-the-future/

[ii] http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/, Wired, accessed 8/12/2016

[iii] https://ripple.com/files/ripple_consensus_whitepaper.pdf, accessed 8/28/2016

[iv] https://www.fincen.gov/news_room/nr/html/20150505.html, accessed 9/7/2016

[v] http://finance.yahoo.com/news/opencoin-extends-ripple-network-bitcoin-120500664.html, accessed 9/

[vi] http://www.gsb.stanford.edu/insights/chris-larsen-money-without-borders, accessed 8/28/2016

[vii] http://www.thebanker.com/Techvision/Ripple-Labs-CEO-looks-to-revolutionise-online-payments?ct=true, accessed 8/10/2016

[viii] Blockchain Decentralizes the Power of Alliances Beyond R3 CEV, accessed 8/10/2016

Copyright Notice

External publication terms for Mercator Advisory Group information and data: Any Mercator Advisory Group information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Mercator Advisory Group research director. A draft of the proposed document should accompany any such request. Mercator Advisory Group reserves the right to deny approval of external usage for any reason.

About Mercator Advisory Group

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver pragmatic and timely research and advice designed to help our clients uncover the most lucrative opportunities to maximize revenue growth and contain costs. Our clients range from the world's largest payment issuers, acquirers, processors, merchants and associations to leading technology providers and investors. Services include *Banking Channels, Credit, Commercial and Enterprise Payments, Debit, Emerging Technologies, International, and Prepaid practices*, which provide research documents and advice; *CustomerMonitor Survey Series*, which report and analyze primary data collected in our biannual consumer surveys; and *Consulting Services*, which enable clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans; offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training. Mercator Advisory Group is also the publisher of the online payments and banking news and information portal PaymentsJournal.com. Visit www.mercatoradvisorygroup.com.

About CO-OP Financial Services

Based in Rancho Cucamonga, Calif., and founded in 1981, CO-OP Financial Services is the nation's largest credit union service organization in terms of number of credit unions and members served. The company helps credit unions compete by providing products and services that make it more convenient for credit union members to do business with their credit unions. With a motto of "Be There. Be More," CO-OP's products and services fall into three business lines, including "Locations," (ATM, shared branching and call center services); "Card Payments" (debit and credit processing) and "Mobile/Virtual" (mobile, online, check imaging, bill pay services). To learn more visit www.co-opfs.org.

About TMG

TMG is dedicated to creating customized payments and processing solutions for financial institutions and the consumers they serve. Driven by a spirit of flexibility and collaboration, TMG tailors innovative credit, debit, ATM, prepaid and digital solutions to the needs of its clients. From patent-pending consumer support technologies to expert guidance on portfolio growth strategies, TMG provides personalized solutions that give clients a competitive advantage in an evolving payments landscape. Simply put, TMG makes life easier for financial institutions and their consumers. To learn more about how TMG creates exceptional client and consumer experiences, visit www.tmg.global